User Manual

TAINY HMOD-V3-IO, TAINY HMOD-L3-IO
TAINY EMOD-V3-IO, TAINY EMOD-L3-IO
Product version DS
Product version E5

Dr. Neuhaus

Copyright Statement

The contents of this publication are protected by copyright. Translations, reprints, reproduction and storage in data processing systems require the express permission of Dr. Neuhaus Telekommunikation GmbH.

© 2015 Dr. Neuhaus Telekommunikation GmbH

All rights reserved.

Dr. Neuhaus Telekommunikation GmbH

Papenreye 65, D-22453 Hamburg

Fax: +49 (40) 55304-180

Internet: http://www.neuhaus.de

E-mail: Kundendienst@neuhaus.de

Subject to technical alterations.

TAINY® is a trademark of Dr. Neuhaus Telekommunikation GmbH. All other trademarks and product designations are trademarks, registered trademarks or product designations of their respective owners.

Dr. Neuhaus Telekommunikation GmbH provides all goods and services on the basis of the General Terms and Conditions of Dr. Neuhaus Telekommunikation GmbH currently valid. All information is based on information provided by the manufacturer(s). No responsibility or liability will be assumed for incorrect or missing entries. The descriptions of the specifications in this manual do not constitute an agreement.

Product no.: 3196

Doc. no.: 3196AD013 version 1.5

Products: TAINY HMOD-V3-IO, TAINY EMOD-V3-IO
TAINY HMOD-L3-IO, TAINY EMOD-L3-IO
incl. product version DS, product version E5
Firmware Version 2.605

Safety instructions

Products

The name TAINY xMOD is used hereinafter as a collective term for TAINY HMOD-V3-IO, TAINY HMOD-L3-IO, TAINY EMOD-V3-IO, and TAINY EMOD-L3- IO as well as the product versions E5 (5-port Ethernet switch) and DS (Dual SIM).

Qualified personnel

The associated device/system may only be set up and operated in conjunction with this documentation. Devices/systems may only be put into service and operated by qualified personnel. For the purposes of the safety instructions in this documentation, qualified personnel are persons who are authorised to put into service, earth and label devices, systems and circuits in accordance with safety engineering standards.

General notes concerning the product

The product TAINY xMOD complies with the European standard EN60950 (11.2006 /A1:2010), Safety of Information Technology Equipment. Read the installation instructions carefully before using the device. Keep the device out of reach of children, especially small children. The device may not be installed or operated outdoors or in damp areas. Do not put the device into operation if connecting cables or the device itself is damaged.

External power supply

Use only an external power supply that also conforms to EN60950. The output voltage of the external power supply must not exceed 60V DC. The output of the external power supply must be short-circuit-proof.

The TAINY xMOD may only be supplied via power supplies according to IEC/EN60950 Section 2.5 "Limited Power Source". The external power supply for the TAINY xMOD must comply with the requirements for NEC Class 2 circuits as defined in the National Electrical Code ® (ANSI/NFPA 70).

When connecting to a battery or rechargeable battery, ensure that an all-pole disconnecting device (battery main switch) with sufficient disconnecting capacity and a fuse with sufficient disconnecting capacity (e.g. Paden FKS fuse set 32 V, 3 A, order no. 162.6185.430) is provided between the device and the battery or rechargeable battery.

Observe the section Technical data of this documentation (Chapter 17) and the instructions for installation and use of the respective manufacturers of the power supply, the battery or the rechargeable battery.

In port and switching output

The in port and switching output are both galvanic insulated against all other terminals of the TAINY xMOD. If the external installation being connected to the TAINY xMOD connects a signal of the in port and switching output galvanically to a power supply signal of the TAINY xMOD, the voltage between each signal of the in port and switching output and each signal of the power supply may not exceed 60V.

Handling cables

Never pull on the cable to pull a cable plug out of its socket; instead pull on the plug. Always use edge protectors when routing cables over sharp corners and edges. Provide adequate strain relief for cables when necessary.

For safety reasons, ensure that the bending radii of the cables are observed.

Failure to observe the bending radii of the antenna cable will degrade the device's transmitting and receiving characteristics. The bending radius must not be less than the minimum of 5 times the cable diameter statically and 15 times the cable diameter dynamically.

Wireless device

Never use the device in areas where the operation of wireless equipment is prohibited. The device contains a wireless transmitter that may degrade the function of electronic medical devices such as hearing aids or pacemakers. Please consult your physician or the manufacturer of such devices. To prevent demagnetisation of data storage media, do not place any floppy disks, credit cards or other magnetic data storage media near the device.

Antenna installation

The recommended radiological limits of the German Commission on Radiological Protection (Strahlenschutzkommission) of 13/14 September 2001 must be complied with.

Installing an outdoor antenna

When installing an antenna outdoors, the antenna must be installed properly by qualified personnel. Lightning protection standard DIN EN 62305 part 1 to 4 in their currently valid version and further standards must be complied with.

The EMC lightning protection zone concept according to DIN EN 62305-4

The EMC lightning protection zone concept must be observed. In order to avoid large induction loops, lightning protection equipotential bonding must be used. If the antenna or the antenna cable is installed in the area of the lightning protection system, then the minimum distances from the lightning protection system must be observed. If this is not possible, then isolated installation as described in lightning protection standard DIN EN 62305 part 1 to 4in their currently valid version is absolutely essential.

RF exposure

Normally the antenna connected to this device's transmitter works in all directions with 0 dB amplification. The composite power in PCS mode is less than 1 watt ERP when this antenna is used.

The internal / external antennas used with this mobile device must be at least 20 cm from persons, and they may not be placed or operated so that they work in a combination with another antenna or transmitter.

Radio interference

The TAINY xMOD is a Class A device. This device can cause radio interference in residential areas; in this case the user may be required to take appropriate measures.

Warning about costs

Please note that data packets which are subject to charges are exchanged even when a connection is (re-) established, when an attempt to connect to a remote station is made (e.g. server is switched off, wrong destination address, etc.), and to maintain a connection.

In example, a remote station which is not available may cause significant unwanted costs, because of a great number of connection retries, being not successful.

Firmware with open source GPL/LGPL

The firmware for TAINY xMOD contains open source software under GPL/LGPL conditions. We provide you with the source code in accordance with Section 3b of GPL and Section 6b of LGPL. You can find the source code on our webpage, www.neuhaus.de.

As an alternative, you can also request the source code from us on CD-ROM. Send your email to Kundendienst@neuhaus.de. Please enter "Open Source xMOD" in the subject line of your email so that we can easily filter out your message.

The license conditions for the open source software can be found in the source code on the product CD.

Firmware with OpenBSD

The firmware of the TAINY xMOD contains parts from the OpenBSD software. Whenever OpenBSD software is used, the following copyright note must be reproduced:

```
* Copyright (c) 1982, 1986, 1990, 1991, 1993
* The Regents of the University of California. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must display the following acknowledgement:
*    This product includes software developed by the University of
*    California, Berkeley and its contributors.
* 4. Neither the name of the University nor the names of its contributors
*    may be used to endorse or promote products derived from this software
*    without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
* CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
* WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
```

A word from our technical service

We, the customer service technicians of Dr. Neuhaus Telekommunikation GmbH, offer you our cordial greetings. If you have any difficulties in putting your new device into operation, we will be your contacts, and will be glad to help you. Even if you have a special or unusual combination of hardware and software, and there is something that you cannot get to work right away, you can always turn to us. Our products' good reputation depends on our customers always being able to get help from a team of experienced specialists, who can also deal with unusual combinations. You can reach us at **Kundendienst@neuhaus.de**.

Environmental protection is also important to us

Maintaining an environment worth living in, i.e. to join ecology and economics in an appropriate way, is one of the most important tasks of our times. We meet this challenge in the following ways:

Quality

Requirements-oriented development and production, firmly rooted in state-of-the-art quality assurance mechanisms, ensure products of the highest quality which can remain in use for a long time.

Return guarantee

We are proud of our products. All the same, we acknowledge that they do not last forever. That is why wherever it is technically possible and feasible we manufacture all of our products of recyclable materials. We guarantee that we will take back any device manufactured by us, send the re-usable parts for recycling, and dispose of the rest in an environmentally friendly manner. Please contact our Service Center

Dr. Neuhaus Telekommunikation GmbH
Service-Zentrum
Messestraße 20,
D-18069 Rostock

Please help us to protect the environment.

Dr. Neuhaus Telekommunikation GmbH

Contents

1 Introduction 10
2 Setup 16
2.1 Step by step 16
2.2 Preconditions for operation 17
2.3 Overview of TAINY xMOD with 2-port Ethernet switch 18
2.4 Overview of TAINY xMOD product version E5 18
2.5 Service button 19
2.6 Operating state indicators 19
2.7 Connections 22
2.8 Inserting the SIM card 25
3 Configuration 26
3.1 Overview 26
3.2 Valid characters for user names, passwords and other inputs 27
3.3 TCP/IP configuration of the network adapter in Windows XP 27
3.4 Establishing a configuration connection 28
3.5 Terminating a configuration connection (Logging out) 31
3.6 Status overview 32
3.7 Configuration procedure 35
3.8 Configuration Profiles 35
3.9 Changing the password 37
3.10 Reboot 38
3.11 Load factory settings 39
3.12 Device identification 39
4 Local interface 40
4.1 Port Configuration 40
4.2 IP addresses of the local interface 41
4.3 DHCP server to local network 41
4.4 DHCP Relay to Local Network 43
4.5 DNS to local network 44
4.6 Local host name 45
4.7 System Time/NTP 45
4.8 Additional internal routes 47
4.9 Advanced Settings for the Local Network 47
5 External interface 49
5.1 Network selection and access parameters for UMTS/GPRS 49
5.2 UMTS/GPRS connection monitoring 54
5.2.1 “List“ Mode 55
5.2.2 “Statistics“ Mode 56
5.3 Host name via DynDNS 60

5.4 Secure DynDNS 61
5.5 NAT – Network address translation 62
5.6 Network status 62
5.6.1 Network status (2G) - TAINY EMOD 63
5.6.2 Network status (2G) - TAINY HMOD 64
5.6.3 Network status (3G) 66
5.7 Volume monitoring 67
5.8 Traffic Priority 69
6 Security functions 70
6.1 MAC Filter 70
6.2 Packet filter 70
6.3 Port forwarding 73
6.4 Advanced security functions 75
6.5 Firewall log 76
7 IPsec-VPN connections 77
7.1 Introduction 77
7.2 IPsec VPN roadwarrior mode 79
7.3 IPsec VPN Standard mode 84
7.4 Loading VPN certificates 91
7.5 Firewall rules for VPN tunnel 92
7.6 Monitoring of VPN connections 93
7.7 Advanced settings for IPsec VPN connections 95
7.8 Status of the VPN connections 96
8 OpenVPN connection 97
8.1 Introduction 97
8.2 Connection settings 98
8.3 Root server certificate 100
8.4 Firewall rules for the OpenVPN connection 100
8.5 Advanced settings for the OpenVPN connections 101
8.6 Port forwarding 103
9 Access 105
9.1 Authentication - Local 105
9.2 Authentication - TACACS+ 105
9.3 Remote access - HTTPS 107
9.4 Remote access - SSH 108
9.5 Remote access via dial-in connection 110
10 Log, update and diagnosis 112
10.1 Log 112
10.2 Remote logging 114
10.3 Snapshot 115
10.4 Hardware information 116
10.5 Firmware information 116

10.6 Execute command 116
10.7 Firmware and system update 117
11 SMS 119
11.1 Overview 119
11.2 Alarm SMS 119
11.3 SMS – SMS over IP 120
12 SNMP 123
12.1 Operation via SNMP 123
12.2 Alarm messages via SNMP traps 126
13 Product version E5 (5 port Ethernet switch) 128
13.1 Overview 128
14 Product version DS (Dual SIM-Card) 129
14.1 Overview 129
15 Profile change 130
15.1 Overview 130
15.2 Configuration 130
16 Small lexicon of routers 132
17 Technical data 144
17.1 TAINY HMOD 144
17.2 TAINY EMOD 146

1 Introduction

Products

This manual provides security instructions and describes the operation and installation of the following products

	VPN Function	HSPA+ / UMTS	E-GPRS	GPRS	CSD
TAINY HMOD-V3-IO	**X**	**X**	**X**	**X**	**X*)**
TAINY HMOD-L3-IO	**-**	**X**	**X**	**X**	**X*)**
TAINY EMOD-V3-IO	**X**	**-**	**X**	**X**	**X**
TAINY EMOD-L3-IO	**-**	**-**	**X**	**X**	**X**

*) Only if not registered to a HSPA+ / UMTS network

and the corresponding product versions DS (Dual SIM) and E5 (5-port Ethernet switch)

Product names used

The following collective terms are used in this manual for the various TAINY product versions:

TAINY xMOD	Collective term for TAINY HMOD-V3-IO, TAINY HMOD-L3-IO, TAINY EMOD-V3-IO, and TAINY EMOD-L3-IO incl. product version E5 and DS.
TAINY HMOD	Collective term for TAINY HMOD-V3-IO and TAINY HMOD-L3-IO incl. product version E5 and DS.
TAINY EMOD	Collective term for TAINY EMOD-V3-IO and TAINY EMOD-L3-IO incl. product version E5 and DS.
TAINY xMOD-V3	Collective term for TAINY HMOD-V3-IO and TAINY EMOD-V3-IO incl. product version E5 and DS.
TAINY xMOD-L3	Collective term for TAINY HMOD-L3-IO and TAINY EMOD-L3-IO incl. product version E5 and DS.

Application

The TAINY xMOD provides a wireless connection to the internet or to a private network.

The TAINY HMOD provides this connection anywhere a UMTS network (Universal Mobile Telecommunication System = 3rd generation mobile communications network) or a GSM network (Global System for Mobile Communication = mobile communications network) which provides IP-based data service is available. For UMTS, this means the HSDPA data service (High-Speed Downlink Packet Access), the HSUPA data service (High-Speed Uplink Packet Access), or the UMTS Data Service- For GSM, this means EGPRS (Enhanced General Packet Radio Service = EDGE) or GPRS (General Packet Radio Service).

For HSDPA and HSUPA the term HSPA+ is used in this manual.

The TAINY EMOD provides this connection anywhere a GSM network (Global System for Mobile Communication = mobile communications network) is available, which provides EGPRS (Enhanced General Packet Radio Service = EDGE) or GPRS (General Packet Radio Service) as a service. This requires a SIM card from a mobile network operator with services activated accordingly.

The TAINY xMOD-L3 connects a locally connected application or entire networks to the internet using wireless IP connections. Direct connection can also be made to an intranet which the external remote stations are

connected to.

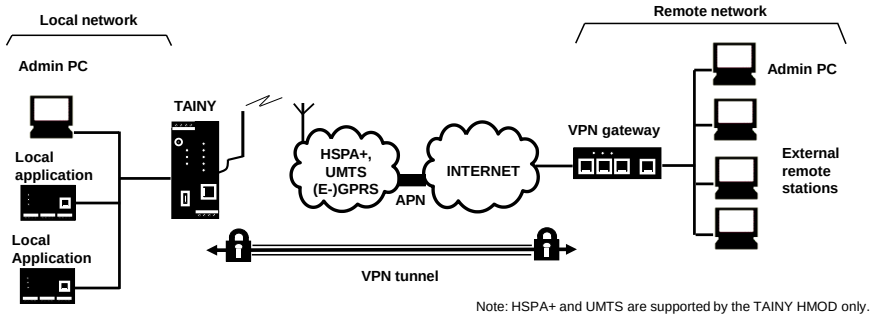
The TAINY xMOD-V3 can establish a VPN (Virtual Private Network) between a locally connected application/network and an external network using a wireless IP connection and can protect this connection from third party access using IPsec (Internet Protocol Security).

The product version DS (Dual SIM) enables alternative operation with a second SIM card, i.e. with a second operator, which takes over the communication if a connection over the first SIM card should be interrupted.

The product version E5 (5-port Ethernet switch) offers three additional Ethernet interfaces for the connection of additional applications to the local network of the TAINY xMOD.

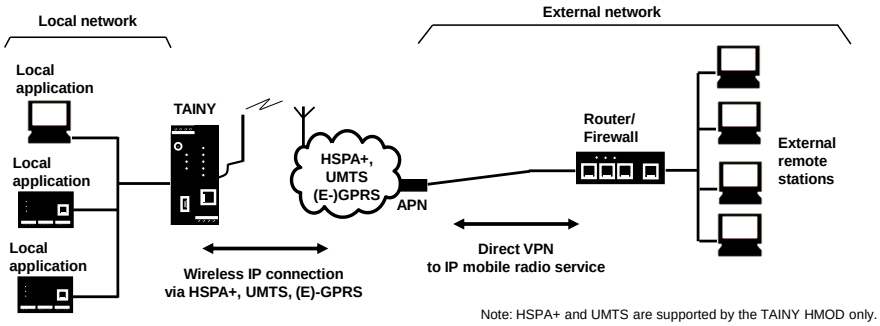
Scenario 1: Virtual Private Network (VPN) with IPsec

TAINY xMOD-V3 only



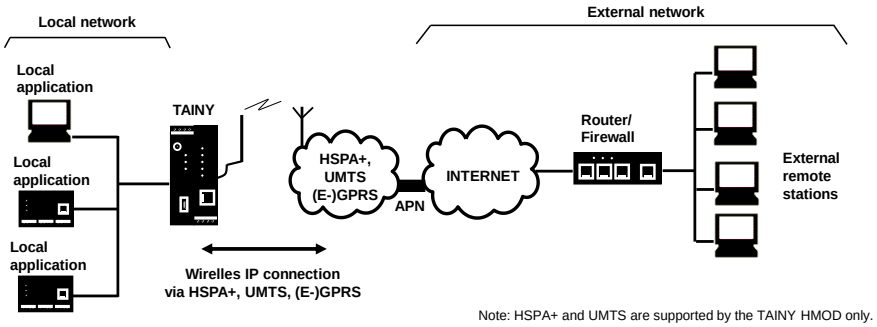
Note: HSPA+ and UMTS are supported by the TAINY HMOD only.

Scenario 2: Connection via HSPA+, UMTS, EGPRS or GPRS and a direct VPN to an external network:



Note: HSPA+ and UMTS are supported by the TAINY HMOD only.

Scenario 3: Connection via HSPA+, UMTS, EGPRS or GPRS and the Internet to an external network:



Note: HSPA+ and UMTS are supported by the TAINY HMOD only.

Local applications could be, for example, a programmable controller, a machine with an Ethernet interface for remote monitoring, or a notebook or desktop PC. These applications use the TAINY xMOD in order to access an external network just as if they had a direct, local connection to this external network.

Functions

In order to perform these tasks in the scenarios described, the device combines the following functions:

	TAINY HMOD		TAINY EMOD	
	V3-IO	L3-IO	V3-IO	L3-IO
HSPA+ / UMTS	X	X	-	-
EGPRS / GPRS / CSD	X*)	X*)	X	X
VPN functions	X	-	X	-
Firewall	X	X	X	X
Configuration	X	X	X	X
Further functions	X	X	X	X

*) Only if not registered to a HSPA+ / UMTS network

This also applies for corresponding devices of the product versions DS and E5.

Communication

Wireless modem for flexible data communication in UMTS networks

- via HSPA+, UMTS

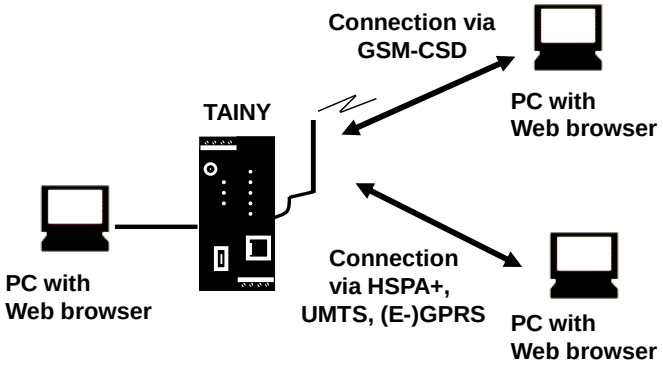
Wireless modem for flexible data communication in GSM networks

- EGPRS, GPRS (and CSD)

Configuration

The device can be configured via a Web user interface that can simply be displayed using a Web browser. It can be accessed by means of the following:

- the local interface,
- HSPA+, UMTS, EGPRS, GPRS, or
- CSD (Circuit Switched Data = dial-in data connection) of the GSM



Note: HSPA+ and UMTS are supported by the TAINY HMOD only.

VPN functions

The TAINY xMOD-V3 provides the following VPN features

- VPN router for secure data transfer via public networks
- Protocol: IPsec (tunnel mode)
- IPsec-3DES encryption with 192 bit
- IPsec-AES encryption with 128, 192 and 256 bit
- Package authentication: MD5, SHA-1
- Internet Key Exchange (IKE) with main and aggressive mode
- Authentication: Pre shared Key (PSK), X.509v3 certificate, CA
- NAT-T
- 1-to-1 NAT
- Dead Peer Detection (DPD)
- Switching output for indicating an established VPN tunnel

OpenVPN functions

- OpenVPN client for secure data transfer via public networks
- Authentication via username, password and Certificate
- LZO compression on the data channel
- Fragmentation of UDP packets
- 1-to-1 NAT
- SNAT

Firewall functions

The TAINY xMOD provides the following firewall functions in order to protect the local network and itself from external attacks:

- Stateful inspection firewall
- Anti-Spoofing
- Port forwarding

Additional functions

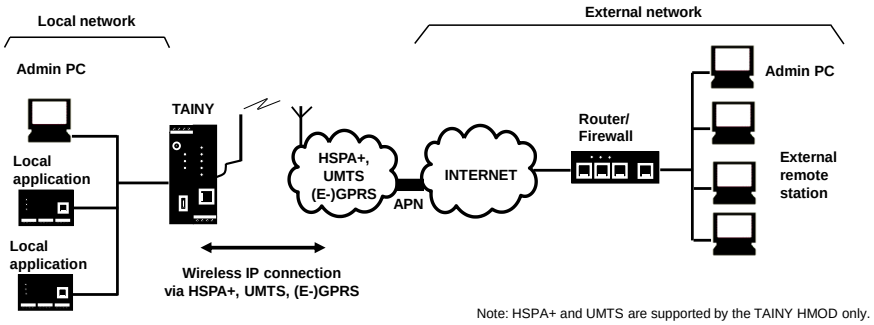
The TAINY xMOD provides the following additional functions:

- Alternative login via TACACS+
- DNS cache
- DHCP server
- NTP
- Remote logging

- In Port
- Web user interface for configuration
- Sending alarm SMSes
- Sending SNMP traps
- Send SMSes from local network
- SSH console for configuration
- SNMP for control and configuration
- DynDNS client
- Dial-in data connection for maintenance and remote configuration
- Data volume control
- Installation mode for antenna alignment

Terms

Here are definitions of terms frequently used in this manual:



Note: HSPA+ and UMTS are supported by the TAINY HMOD only.

Local network	Network connected to the local interface of the TAINY xMOD. The local network contains at least one local application.
Local interfaces LAN 0, LAN 1, LAN 2, LAN 3, LAN 4 (10/100-Base-T)	Interfaces of the TAINY xMOD for connecting the local network. The interfaces are labelled LAN 0 and LAN 1 (10/100 Base-T) on the device. These are Ethernet interfaces with a data rate of 10Mbit/s or 100Mbit/s (Autosensing MDI/MDIX). The TAINY xMOD acts as a switch between the two interfaces. Devices of the product version E5 also have three additional technically identical Ethernet interfaces, which are identified as LAN 2 to LAN 4.
Local application	Local applications are network components in the local network, for example a programmable controller, a machine with an Ethernet interface for remote monitoring, or a notebook or desktop PC or the Admin PC.
Admin PC	Computer with Web browser (e.g. MS Internet Explorer Version 7 or later or Mozilla Firefox Version 2 or later) connected to the local network or the external network; used to configure the TAINY xMOD. The Web browser must support HTTPS. Device configuration via SSH requires an SSH client on the Admin PC, for example putty.

External network

External network which the TAINY HMOD is connected to via HSPA+, UMTS, EGPRS or GPRS. External networks are the internet or a private intranet.

External network which the TAINY EMOD is connected to via EGPRS or GPRS. External networks are the internet or a private intranet.

External remote stations

External remote stations are network components in an external network, e.g. Web servers on the Internet, routers on an intranet, a central company server, an Admin PC, and much more.

(E-)GPRS

EGPRS or GPRS depending on what services are available.

VPN gateway

Component of the external remote network that supports IPsec and which is compatible with the TAINY xMOD-V3.

Remote network

External network with which the TAINY xMOD-V3 is establishing a VPN connection.

Mobile communications network

Infrastructure and technology for wireless mobile verbal and data communication.

The TAINY HMOD is designed for use in UMTS mobile communications networks and GSM mobile communications networks,

The TAINY EMOD is designed for use in EDGE/GSM mobile communications networks.

Mobile data service

Data transmission services provided by the mobile communications network which can be used by the TAINY xMOD:

	TAINY HMOD		TAINY EMOD	
	V3-IO	L3-IO	V3-IO	L3-IO
UMTS wireless net	X	X	-	-
HSPA+	X	X	-	-
UMTS data	X	X	-	-
GSM wireless net (with EDGE)	X	X	X	X
E-GPRS	X	X	X	X
GPRS	X	X	X	X
CSD	X*)	X*)	X	X

*) Only if not registered to a HSPA+ / UMTS network

This also applies for corresponding devices of the product versions DS and E5.

2 Setup

2.1 Step by step

Set up the TAINY xMOD in the following steps:

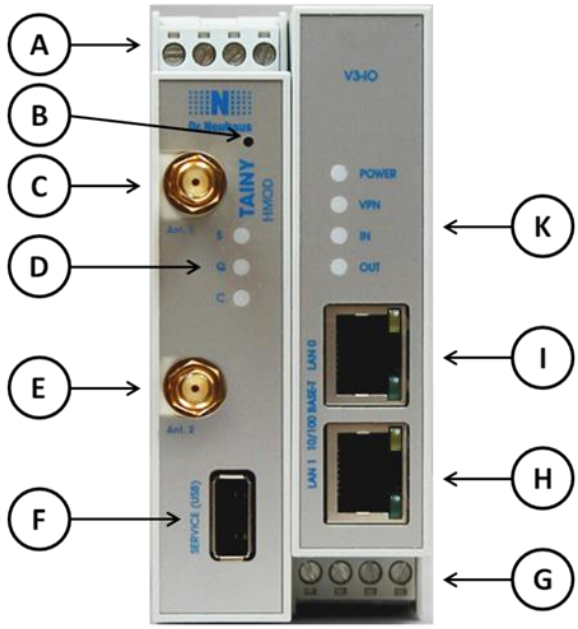
Step		Chapter
1.	First familiarise yourself with the preconditions for operation of the TAINY xMOD.	2.2
2.	Read the safety instructions and other instructions at the beginning of this user manual very carefully, and be sure to follow them.	
3.	Please familiarise yourself with the control elements, connections and operating state indicators of the TAINY xMOD.	2.3 to 2.7
4.	Connect a PC with a Web browser (Admin PC) to one of the local interfaces (10/100 BASE-T) of the TAINY xMOD.	3.3, 3.4
5.	Using the Web user interface of the TAINY xMOD, enter the PIN(s) (Personal Identification Number) of the SIM card(s).	5.1
6.	Disconnect the TAINY xMOD from the power supply.	2.7
7.	Insert the SIM card(s) in the device.	2.8
8.	Connect the antenna(s).	2.7
9.	Connect the TAINY xMOD to the power supply.	2.7
10.	Set the TAINY xMOD up in accordance with your requirements.	3 to 15.2
11.	Connect your local application.	2.7

2.2 Preconditions for operation

In order to operate the TAINY xMOD, the following information must be on hand and the following preconditions must be fulfilled:

Antenna	An antenna, adapted to the frequency bands of the GSM network operator you have chosen: 850 MHz, 900 MHz, 1800 MHz or 1900 MHz. Please use only antennas from the accessories for the TAINY xMOD, because they are tested to operate together with the TAINY xMOD. See Chapter 2.7.
Power supply	A power supply with a voltage between 12 V_{DC} and 60 V_{DC} that can provide sufficient current (I_{Burst}>1.26 A). See Chapter 2.7 and 17.
SIM card	A SIM card from the chosen GSM network operator.
PIN	The PIN for the SIM card
HSPA+ / UMTS EGPRS / GPRS activation	The services HSPA+, UMTS data (only TAINY HMOD) and / or EGPRS or GPRS must be enabled on the SIM card by your mobile communications network provider. The access data must be known: - Access Point Name (APN) - User name - Password
CSD 9600 bit/s activation	The SIM card must be activated by your GSM network operator for the CSD service if you wish to use remote configuration via a dial-in data connection, see Chapter 9.5.

2.3 Overview of TAINY xMOD with 2-port Ethernet switch



A – Connection terminals for the power supply

B – Service button

C – Antenna jack 1, type SMA

D – Operating state indicators S, Q, C

E - Antenna jack 2, type SMA (only TAINY HMOD-x3-IO)

F – Service (USB) – Reserved for future applications

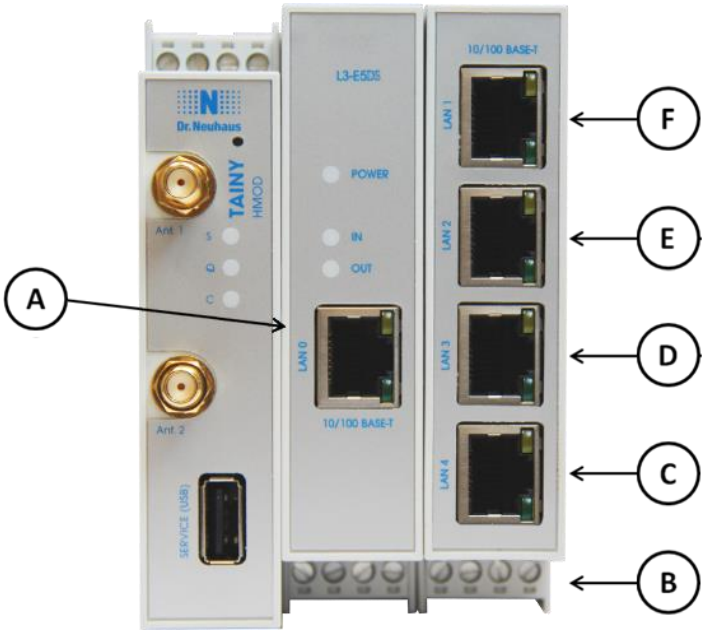
G – Connection terminals for the gate inputs and outputs

H – LAN0 / 10/100-Base-T
RJ45 jack for connecting the local network with integrated indicator lamps

I – LAN1 / 10/100-Base-T
RJ45 jack for connecting the local network with integrated indicator lamps

K – Operating state indicators
POWER, IN, OUT
VPN (only TAINY xMOD-V3)

2.4 Overview of TAINY xMOD product version E5



A – LAN0 / 10/100-Base-T - RJ45 jack for connecting the local network with integrated indicator lamps

B – Connection terminals – reserved for later use

C – LAN4 / 10/100-Base-T - RJ45 jack for connecting the local network with integrated indicator lamps

D – LAN3 / 10/100-Base-T - RJ45 jack for connecting the local network with integrated indicator lamps

E - LAN2 / 10/100-Base-T - RJ45 jack for connecting the local network with integrated indicator lamps

F – LAN1 / 10/100-Base-T - RJ45 jack for connecting the local network with integrated indicator lamps

2.5 Service button

On the front side of the TAINY xMOD there is a small hole (see Chapter 2.3, B) which has a button behind it. Use a pointed object, e.g. a straightened-out paperclip, to press this button.

- If you press the button for longer than 5 seconds, the TAINY xMOD reboots and loads the factory settings.

2.6 Operating state indicators

The TAINY xMOD-V3 has seven indicator lamps (LEDs), while the TAINY xMOD-L3 has six indicator lamps (LEDs) for displaying the operating status. In addition there are two integrated indicator lamps each in the connections LAN 0 and LAN 1 or LAN 0 to LAN 4 with the product version E5.

The three indicator lamps on the left half of the device indicate the status of the wireless modem:

TAINY HMOD

Lamp	State	Meaning
S *(Status)*	Flashing slowly	PIN transfer
	Flashing quickly	PIN error / SIM error
	ON	PIN transfer successful
Q *(Quality)*	OFF	Not logged into GSM network
	Flashing briefly	Poor signal strength (CSQ < 6)
	Flashing slowly	Medium signal strength (CSQ = 6.. 10)
	ON, with brief interruptions	Good signal strength (CSQ = 11.. 18)
	ON	Very good signal strength (CSQ > 18)
C *(Connect)*	OFF	No connection
	Flashing quickly	Service call via CSD active
	Flashing slowly	EGPRS / GPRS connection active
	ON	HSPA+ / UMTS connection active
S, Q, C together	Light up in sequence quickly	Booting
	Light up in sequence slowly	Update
	Flashing quickly in unison	Error

TAINY EMOD

Lamp	Status	Meaning
S *(Status)*	Flashing slowly	PIN transfer
	Flashing quickly	PIN error / SIM error
	ON	PIN transfer successful
Q *(Quality)*	OFF	Not logged into GSM network
	Flashing briefly	Poor signal strength (CWQ < 6)
	Flashing slowly	Medium signal strength (CSQ = 6.. 10)
	ON with brief interruptions	Good signal strength (CSQ = 11.. 18)
	ON	Very good signal strength (CSQ > 18)
C *(Connect)*	OFF	No connection
	Flashing quickly	Service call via CSD active
	ON with brief interruptions	GPRS connection active
	ON	EGPRS connection active
S, Q, C together	Light up in sequence quickly	Booting
	Light up in sequence slowly	Update
	Flashing quickly in unison	Error

TAINY xMOD-V3

The four indicator lamps on the right-hand side (product version IO) or the middle section (product version E5) of the device indicate the state of additional device functions:

Lamp	State	Meaning
POWER	ON	Device switched on, operating voltage present
	OFF	Device switched off, operating voltage not present
VPN	ON	At least one VPN connection established
	OFF	No VPN connection established
IN	ON	In port active
	OFF	In port not active
OUT	ON	If the switching output is active.
	OFF	If the switching output is not active.

TAINY xMOD-L3

The three indicator lamps on the right-hand side (product version IO) or the middle section (product version E5) of the device indicate the following additional device functions:

Lamp	Status	Meaning
POWER	ON	Device switched on, operating voltage present
	OFF	Device switched off, operating voltage not present
IN	ON	Switching input active
	OFF	Switching input not active
OUT	ON	Reserved for future applications
	OFF	Reserved for future applications

Indicator lamps at the Ethernet sockets (2-port version)

The indicator lamps at LAN 0 and LAN 1 (product version IO) show the status of the corresponding connection:

Lamp	Status	Meaning
LAN 0-1, Green	OFF	Ethernet link not detected
	ON	Ethernet link detected
LAN 0-1, Yellow	OFF	No data transfer
	Flashing	Data transfer

Indicator lamps at the Ethernet sockets (5-port version)

The indicator lamps at LAN 0 to LAN 4 (product version E5) show the status of the corresponding connection:

Lamp	Status	Meaning
LAN 0-4, Green	OFF	Ethernet link not detected
	ON	Ethernet link detected
LAN 0, Yellow	OFF	No data transfer
	Flashing	Data transfer
LAN 1-4, Yellow	ON	No data transfer
	Flashing	Data transfer

2.7 Connections

LAN 0 - LAN 4 (10/100 Base-T)

The sockets LAN0 or LAN1 (10/100 Base-T, with the product version E5, LAN 0 to LAN 4) are used to connect the local network with local applications e.g. a programmable controller, a machine with an Ethernet interface for remote monitoring, or a notebook or desktop PC.

The TAINY xMOD acts as a switch between the available interfaces.

To set up the TAINY xMOD, connect the Admin PC with Web browser here.

The interfaces support auto negotiation. It is thus detected automatically whether a transmission speed of 10 Mbit/s or 100 Mbit/s is used on the Ethernet.

A connecting cable with a RJ45 plug must be used. It can be wired cross-over or one-to-one.

Service (USB)

In the TAINY xMOD this interface has no function and is reserved for later applications. Please do not connect any devices here. Doing so could interfere with the TAINY xMOD operation.

SMA antenna jacks

The TAINY HMOD has two SMA type antenna jacks to connect antennas; the TAINY EMOD has one SMA type antenna jack to connect an antenna.

Please make sure, that in operation always at least one antenna is connected to the TAINY HMOD as well as to the TAINY EMOD. The antenna jack Ant 1 of a TAINY HMOD must be used.

A second antenna can be connected to antenna jack Ant 2 of the TAINY HMOD to improve the receiver performance.

The antennas that are used should have an impedance of about 50 ohms. It must be matched for GSM 900MHz, DCS 1800MHz, UMTS 2100MHz or GSM 850 MHz and PCS 1900 MHz, depending on which frequency bands your mobile radio network operator uses. In Europe and China GSM 900MHz and DCS 1800MHz are used for GSM and 2100 MHz is used for UMTS, in the USA GSM 850 MHz and PCS 1900 MHz are used for GSM and UMTS. Please obtain this information from your network operator.

The matching (VSWR) of the antenna must be 1:2.5 or better.

Caution:

Please use only antennas from the accessories line for TAINY xMOD. Other antennas could interfere with product characteristics or even lead to defects.

When installing the antenna, a sufficiently good signal quality must be ensured (CSQ > 11). Use the indicator lamps of the TAINY xMOD which show the signal quality or the webpage *Network status*, see chapter 5.6. Please make sure that there are no large metal objects (e.g. reinforced concrete) close to the antenna.

The second antenna of the TAINY HMOD should be installed at a distance of 30 to 100cm from the first aerial.

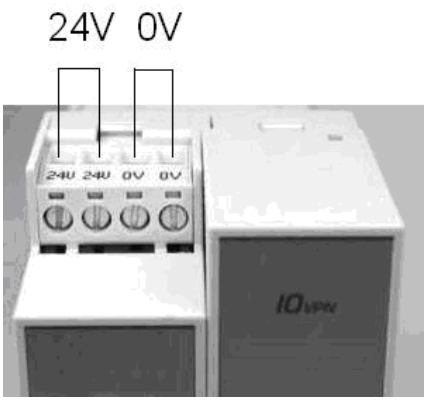
Please observe the installation and user instructions for the antenna being used.

Warning:

When the antenna is installed outdoors it must be earthed for lightning protection. This work must be carried out by qualified personnel.

Screw terminals

Power supply



In port and switching output

24V / 0V power supply

The TAINY xMOD operates with direct current of from 12-60 V DC, nominally 24 V DC. This power supply is connected at the screw terminals on the left-hand side of the device.

The current consumption is about 450mA at 12V and 100mA at 60V (I_{Burst}>1.26 A).

Warning:

The power supply unit of the TAINY HMOD-V3-IO is not isolated.

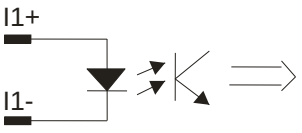
Please observe the safety instructions at the beginning of this manual.

Note:

Make sure that the supply source is sufficiently dimensioned. Instable operation may occur if the supply is too weak.

In port
I1+/ I1-

The TAINY xMOD has an In port. The In port has connections at the screw terminals on the right-hand side of the device. The terminals are designated I1+/I1-.



U_{In} = 5 …30V; ON: $U_{In} \geq$ 5 V; OFF: $U_{In} \leq$ 1,2 V

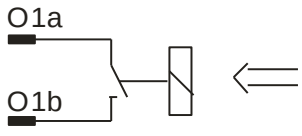
For more on the function of the In port, see also Chapter 11.

Warning:

The In port is galvanically insulated against all other terminals of the TAINY xMOD. If the external installation being connected to the TAINY xMOD connects a signal of the In port galvanically to a power supply signal of the TAINY xMOD, the voltage between each signal of the In port and each signal of the power supply may not exceed 60V.

Switching output O1a/ O1b

The TAINY xMOD-V3 has a switching output. The switching output has its connections at the screw terminals on the right-hand side of the device or the middle section with the product version E5. The terminals are designated O1a/O1b.



U_{Max} = 30 V; I_{Max} = 20 mA

The switching output is active (switch closed) if at least one VPN connection is established.

The switching output is not active (switch opened) if no VPN connection is established.

Warning:

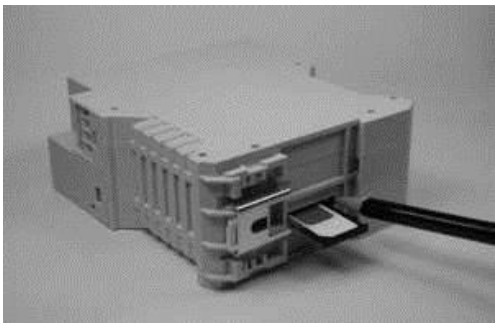
The switching output is galvanically insulated against all other terminals of the TAINY xMOD. If the external installation being connected to the TAINY xMOD connects a signal of the switching output galvanically to a power supply signal of the TAINY xMOD, the voltage between each signal of the switching output and each signal of the power supply may not exceed 60V.

Additional terminal block of the product version E5

Devices of the product version E5 have an additional 4-pole screw terminal block in the right section.

This interface has no function with the TAINY xMOD and is reserved for later applications. Please do not connect any devices here. This could result in a malfunction of the TAINY xMOD.

2.8 Inserting the SIM card



Caution:

Before inserting the SIM card, enter the PIN of the SIM card in the TAINY xMOD via the Web user interface. See Chapter 5.1

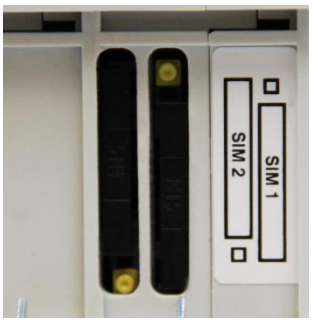
1. After you have entered the PIN of the SIM card, disconnect the TAINY xMOD completely from the power supply.
2. The drawer for the SIM card is located on the back of the device. Right next to the drawer for the SIM card in the housing aperture there is a small yellow button. Press on this button with a pointed object, for example a pencil.

   When the button is pressed the SIM card drawer comes out of the housing.
3. Place the SIM card in the drawer so that its gold-plated contacts remain visible.
4. Then push the drawer with the SIM card completely into the housing.

Caution!

Do not under any circumstances insert or remove the SIM card during operation. Doing so could damage the SIM card and the TAINY xMOD.

ONLY PRODUCT VERSION DS



Devices of the product version DS have a second opening for an additional SIM card tray on the rear side of the device. Please observe the instructions above when inserting the second SIM card.

3 Configuration

3.1 Overview

Configuration of the router and firewall functions is carried out locally or remotely via the Web-based administration interface of the TAINY xMOD. The VPN function can also be configured for the TAINY xMOD-V3.

Remote configuration

Remote configuration via HTTPS or CSD access is only possible if the TAINY xMOD is configured for remote access. In this case proceed exactly as described in Chapter 7.

Configuration via the local interface

The preconditions for the initial configuration via the local interface are:

- The computer (Admin PC) that you use to carry out configuration must be either:
  - connected directly to the Ethernet jack of TAINY xMOD via a network cable

  or
  - it must have direct access to the TAINY xMOD via the local network.
- The network adapter of the computer (Admin PC) that you use to carry out configuration must have the following TCP/IP configuration:

  IP address: **192.168.1.2**

  Subnet mask: **255.255.255.0**

  Instead of the IP address **192.168.1.2** you can also use other IP addresses from the **range 192.168.1.x**. but not 192.168.1.1, 192.168.1.0 und 192.168.1.255.
- If you also wish to use the Admin PC to access the external network via the TAINY xMOD, the following additional settings are necessary:

  Standard gateway: **192.168.1.1**

  Preferred DNS server: **Address of the domain name server**

3.2 Valid characters for user names, passwords and other inputs

Valid characters

For user names, passwords, host names, APN and PIN the following ASCII characters may be used:

User names and passwords	@ ~ % $, * ' = ! + - \ / ? ( ) { } . : ; [ ] _ | 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z
	For access parameters for UMTS/GPRS (see Chap. 5.1) also use the # character can be used.
host names and APN	. - 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z
PIN	PINs support numeric characters only 0 1 2 3 4 5 6 7 8 9

Some parameters accept additional special characters.

3.3 TCP/IP configuration of the network adapter in Windows XP

Windows Connect To…

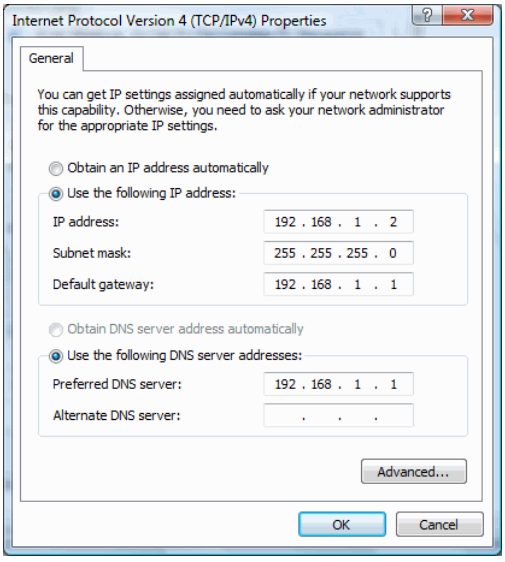
Click on *Start, Connect To ..., Show All Connections…*

Then click on *LAN Connection.* In the dialog box *Properties of LAN Connection*, click on the *General* tab and select there the entry *Internet Protocol (TCP/IP).* Open *Properties* by clicking on the corresponding button.

The window *Properties of Internet Protocol (TCP/IP)* appears (see illustration below).

Note:

The path leading to the dialog box *Properties of LAN Connection* depends on your Windows settings. If you are not able to find this dialog box, please search in the Windows Help function for *LAN Connection* or *Properties of Internet Protocol (TCP/IP)*.



Enter the following values in order to get to the Web user interface of the TAINY xMOD:

IP address: **192.168.1.2**

Subnet mask: **255.255.255.0**

In addition, enter the following values if you want to use the Admin PC to access the external network via the TAINY xMOD:

Standard gateway: **192.168.1.1**

Preferred DNS server: **Address of the Domain Name Servers**

Preferred DNS server

If you call up addresses via a domain name (e.g. www.neuhaus.de), then you must refer to a domain name server (DNS) to find out what IP address is behind the name. You can define the following as the domain name server:

- The DNS address of the network operator,

  or

- The local IP address of the TAINY xMOD, as long as it is configured for breaking out host names into IP addresses (see Chapter 4.4). This is the **factory setting**.

  To define the domain name server in the TCP/IP configuration of your network adapter, proceed as described above.

3.4 Establishing a configuration connection

Setting up a Web browser

Proceed as follows:

Launch a Web browser (e.g. MS Internet Explorer Version 7 or later or Mozilla Firefox Version 2 or later; the Web browser must support SSL (i.e. HTTPS).).

Make sure that the browser does not automatically dial a connection when it is launched.

In MS Internet Explorer 7, make this setting as follows: Menu *Tools, Internet Options...*, tab *Connections*: The option *Do not select a connection* must be activated.

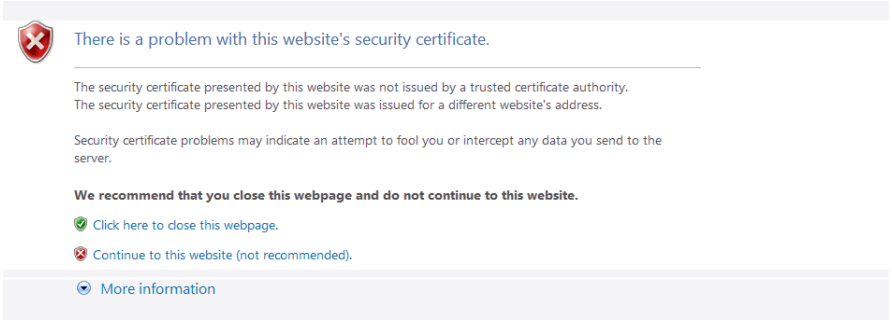
Calling up the start page of the TAINY xMOD

In the address line of the browser, enter the address of the TAINY xMOD in full. In the factory settings this is:

https://192.168.1.1

Result: A security message appears. In Internet Explorer 7, for example, this one:

Confirming the security message



Acknowledge the corresponding safety message with "Continue loading this page …"

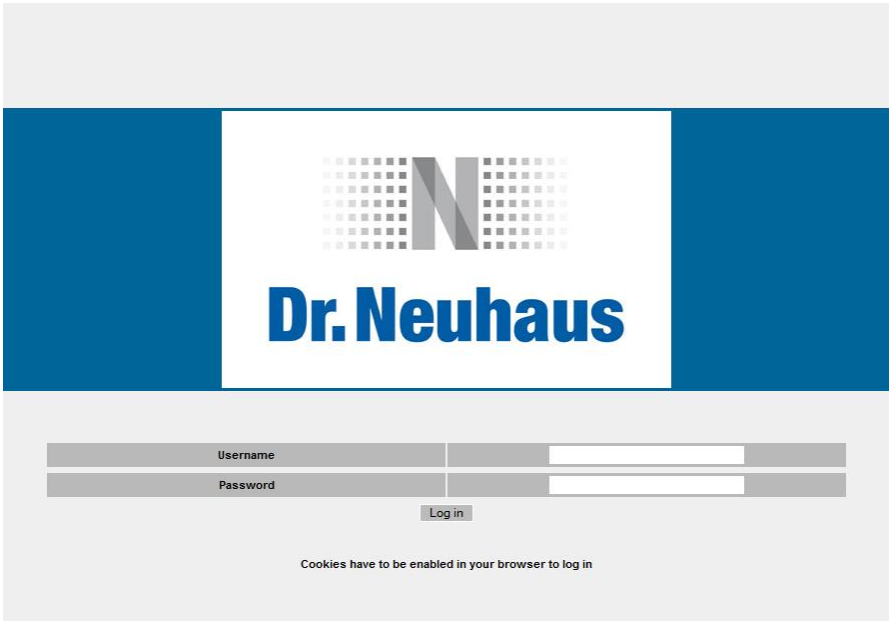
Note

Because the device can only be administered via encrypted access, it is delivered with a self-signed certificate. In the case of certificates with signatures that the operating system does not know, a security message is generated. You can display the certificate.

It must be clear from the certificate that it was issued for Dr. Neuhaus Telekommunikation GmbH. The Web user interface is addressed via an IP address and not using a name, which is why the name specified in the security certificate, is not the same as the one in the certificate.

You will be asked to enter the user name and the password:

Entering the user name and password



The factory setting is:

User name: **root**

Password: **root**

Note

You should change the password in any event. The factory setting is general knowledge and does not provide sufficient protection. Capital 3.9 contains a description of how to change the password.

Note

To enable you to register successfully on the TAINY xMOD, you have to activate cookies in your browser.

Note

If the authentication via TACACS+ is already activated in TAINY xMOD, the registration screen also shows a selection menu, where the registration can take place via TACACS+ or the normal, local registration. The local registration process is described below first of all, which is used when commissioning the device. For further information on registration via TACACS+, see 9.2.

The start page is displayed

After the user name and password are entered, the start page of the TAINY xMOD appears in the Web browser with an overview of the operating state, see Chapter 3.6.

The start page is **not** displayed

If after several tries the browser still reports that the page cannot be displayed, try the following:

- Check the hardware connection. On a Windows computer, go to the DOS prompt (Menu *Start, Programs, Accessories, Command Prompt*) and enter the following command:

  ping 192.168.1.1

  If a return receipt message for the 4 packets that were sent out does not appear within the specified time period, please check the cable, the connections and the network card.

- Make sure that the browser does not use a proxy server. In MS Internet Explorer (Version 7.0), make this setting as follows: Menu *Tools, Internet Options...*, tab *Connections*: Under *LAN Settings*, click on the *Settings...* button, then in the dialog box *Settings for local network (LAN)*, make sure that under *Proxy Server* the entry *Use proxy server for LAN* is not activated.

- If other LAN connections are active on the computer, deactivate them for the duration of the configuration process.
  Under the Windows menu *Start, Connect To ..., Show All Connections…*, under LAN or High-Speed Internet right-click on the connection concerned and select *Deactivate* in the pop-up menu.

- Enter the address of the TAINY xMOD with a slash:

  https://192.168.1.1/

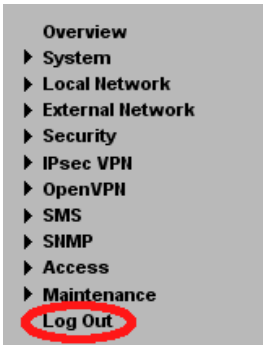
3.5 Terminating a configuration connection (Logging out)

Log Out

Use the menu item *Log Out* to sign out manually. This will terminate the configuration connection to your TAINY xMOD. The webserver will return to the start screen.

In order to re-establish the configuration connection, you have to enter user name and password again.

Please refer to chapter 3.4.

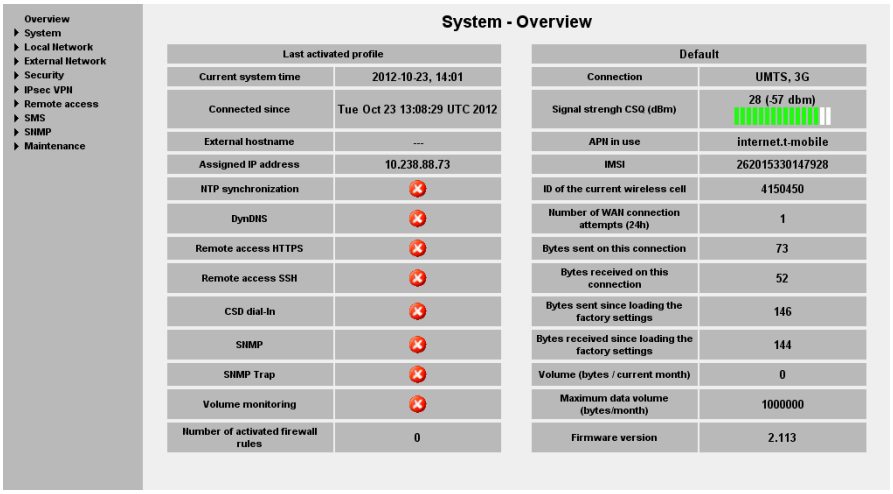


Note

If the configuration connection stays idle for at least 15 min, the device terminates the connection automatically. On the next access to one of the TAINY xMOD's websites the web server returns to the start screen. Please refer to chapter 3.4 on how to re-establish a configuration connection.

3.6 Status overview

Overview



After the Web user interface of the TAINY xMOD is called up and the user name and password are entered, an overview of the current operating state of the TAINY xMOD appears.

Note

Use the *Refresh* function of the web browser to update the displayed values.

Last activated profile — Displays the name of the latest activated configuration profile

Note

The content of this profile does not have to be necessarily identical to the parameter values currently activated in the TAINY xMOD. In case there have been changes to the configuration after the profile shown here has been activated, the current configuration of the TAINY and the profile will differ.

Current system time — Displays the TAINY xMOD's current system time in the format:

Year – Month – Day, Hours – Minutes

Connected since — Shows the time stamp, when the current connection to the mobile data service has been established.

External host name — Displays the TAINY xMOD's host names (e.g. tainy.mydns.org), if a DynDNS service is used.

Assigned IP address — Shows the IP address which the TAINY xMOD can be reached at through the mobile data service. This IP address is assigned to the TAINY xMOD by the mobile data service.

Connection — Indicates if and which wireless connection is established.

For TAINY HMOD:

- UMTS connection (IP connection via HSPA+, UMTS data)
- GPRS/EDGE connection (IP connection via EGPRS or GPRS)
- CSD connection (service connection via CSD)

For TAINY EMOD:

- EDGE connection (IP connection via EGPRS)
- GPRS connection (IP connection via GPRS)

- CSD connection (service connection via CSD)

In case of some certain connection problem, related messages are shown here.

Note

It is possible that a wireless connection and an assigned IP address are displayed, but the connection quality is not good enough to transmit data. For this reason, we recommend using the active connection monitoring (see chapter 5.2).

Signal strength CSQ (dBm)

Indicates the strength of the GSM signal as a CSQ value and (in parentheses) as an RSSI value in dBm.

- CSQ = 0: No connection to the mobile network
- CSQ < 6: Poor signal strength
- CSQ = 6..10: Medium signal strength
- CSQ = 11..18: Good signal strength
- CSQ > 18: Very good signal strength

APN in use

Shows the APN (= Access Point Name) used for the mobile data service.

IMSI

Shows the participant recognition, which is stored on the SIM card in use.

The GSM network operator recognises the SIM card's authorisations and agreed services based on the IMSI (= International Mobile Subscriber Identity).

NTP synchronization

Shows whether the NTP synchronization is activated

NTP synchronization activated.

NTP synchronization not activated.

DynDNS

Shows whether a DynDNS service is activated

DynDNS service activated.

DynDNS service not activated

Remote access HTTPS

Shows whether remote access to the Web user interface of the TAINY xMOD via mobile radio network is permitted (see Chapter 9.1).

Access using HTTPS is allowed.

Access using HTTPS is not allowed.

Remote access SSH

Shows whether remote access to the SSH console of the TAINY HMOD-V3-IO via mobile radio network is permitted (see Chapter 9.4).

Access using SSH is allowed.

Access using SSH is not allowed.

Remote access CSD Dial-In

Shows whether remote CSD service calls are allowed (see Chapter 9.5).

CSD service calls are allowed.

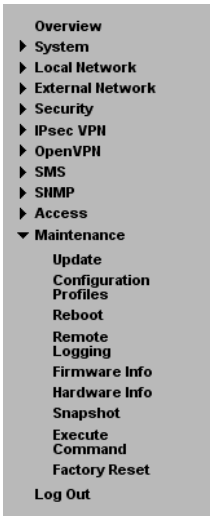
	CSD service calls are not allowed.
SNMP	Shows whether the setting and reading of parameters via SNMP is enabled (see chapter 12.1): Setting/reading of parameters via SNMP is allowed. Setting/reading of parameters via SNMP is not allowed.
SNMP Trap	Shows whether the sending of SNMP messages (SNMP traps) is enabled (see chapter 12.2): Sending of SNMP messages activated. SNMP messages not activated.
Volume monitoring	Shows whether the traffic volume supervision is switched on (see chapter 5.7): Traffic volume supervision is activated. Traffic volume supervision is not activated.
ID of the current wireless cell	Shows the identification of mobile network base station which the TAINY xMOD is currently connected to.
Number of WAN connection attempts (24h)	Shows the TAINY xMOD's number of login attempts to the APN since 0:00 (system time). The value 0 indicates that no repeat login attempts have taken place.
Bytes sent / Bytes received on this connection	Shows the number of bytes which have been sent or received during the present connection via the mobile data service. The counter is reset when a new connection is established. **Note** These figures merely serve as an indication of the data volume and may deviate from the calculation of the network operator.
Bytes sent / Bytes received since loading the factory settings	Shows the number of bytes which have been sent or received via the mobile data service since the factory settings were most recently loaded. The counters are reset when the factory settings are loaded.
Volume (bytes / current month)	Shows the number of bytes sent and received since the beginning of the month (system time). **Note** These figures merely serve as an indication of the data volume and may deviate significantly from the calculation of the GSM network operator. The NTP synchronization must be activated.
Maximum data volume (bytes/month)	Shows the warning level set for the data volume, at which point the TAINY xMOD sends a message.
Number of activated firewall rules	Shows how many firewall rules are activated.
Firmware version	Shows the version number of the TAINY xMOD's software.

3.7 Configuration procedure

The procedure for configuration is as follows:

Carrying out configuration

1. Use the menu to call up the desired settings area
2. Make the desired entries on the page concerned or use **Reset** to delete the current entry which has not been saved.
3. Use **Save** to confirm the entries so that they are accepted by the device.



ONLY TAINY xMOD-V3

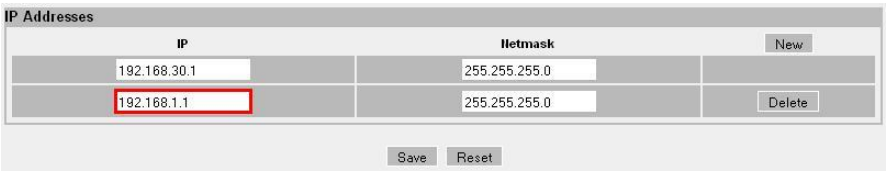
Note regarding the scope of function

The menu item IPsec-VPN is only present for the TAINY xMOD-V3 devices.

- Depending on how you configure the TAINY xMOD, you may then have to adapt the network interface of the locally connected computer or network accordingly.
- When entering IP addresses, always enter the IP address component numbers without leading zeros, e.g.: 192.168.0.8.

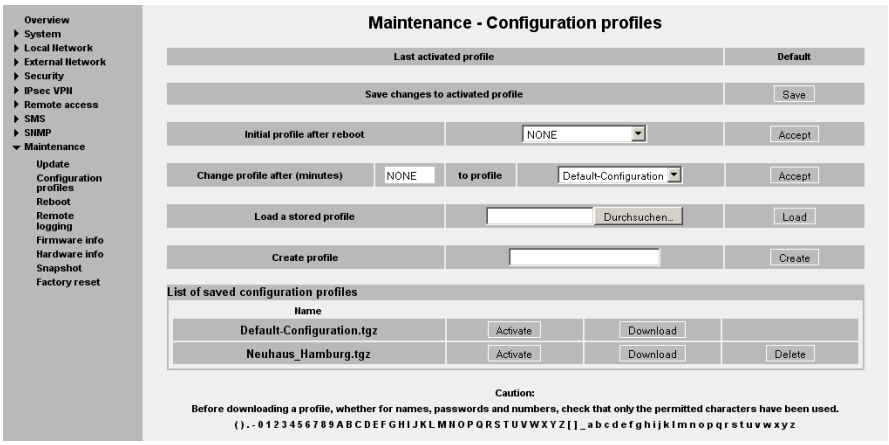
Invalid entries

The TAINY xMOD checks your entries. Obvious errors are detected during saving and the input box in question is marked. The entered value is reset to the default value.



3.8 Configuration Profiles

Maintenance > Configuration Profiles



Function	The settings of the TAINY xMOD can be saved in configuration profiles (files) and re-loaded at any time.
Last activated profile	Displays the name of the latest activated configuration profile. If no profile has been activated since bringing the TAINY xMOD into service or if the device has been reset to factory settings (see chapter 3.11) the display reads *Default*.
Save changes to activated profile	Saving changes in the configuration by using the *Save* buttons on the respective pages in the web user interface affects the currently used configuration of the TAINY xMOD only, not the configuration profile shown as *Last activated profile*. As soon as a configuration profile is activated these changes will be discarded. The Button *Save changes to activated profile* writes configuration changes to the *Last activated profile*.
Initial profile after reboot	Select the configuration profile from the profiles stored in the TAINY xMOD that will be activated after the next reboot of the device here. If *NONE* is selected the device starts with the same configuration that was active before the restart.
Change profile after (minutes)	The TAINY xMOD supports time-scheduled profile changes. The respective parameters have the following meaning: *Change profile after (minutes)* — Define the interval (in minutes) for the time-controlled profile change here *to profile* — Select the configuration profile from the profiles stored in the TAINY xMOD that will be activated after the interval *Change profile after (minutes)* has elapsed here.
Load a stored profile	Loads to the TAINY xMOD a configuration profile that was created before and saved on the Admin PC. Files with configuration profiles have the file extension *.tgz. *Browse* can be used to search the Admin PC for configuration profiles, *Load* submits the configuration profile to the TAINY xMOD. It will then be shown in the table of saved configuration profiles.
Create profile	Saves the current settings of the TAINY xMOD in a configuration profile. First enter a name for the profile in the input box. *Create* saves the settings in a profile with this names and then displays them in the table of saved configuration profiles. The following characters may be used for the name: ( ) . - 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ ] _ a b c d e f g h i j k l m n o p q r s t u v w x y z *Create* saves the settings in a profile with this name and then shows them in the table of saved configuration profiles.
List of saved configuration profiles	The list of saved configuration profiles shows all of the profiles that are stored in the TAINY xMOD. *Download* — Loads the profile to the Admin PC. *Activate* — The TAINY xMOD accepts the settings from the selected configuration profile and continues to work using them. *Delete* — The configuration profile is deleted.

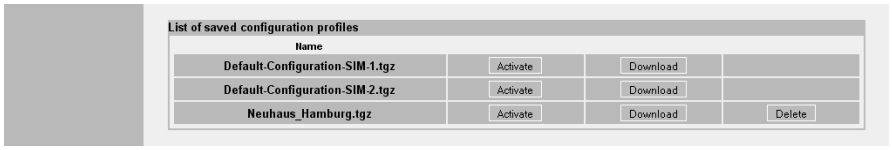
The profile *Default-Configuration.tgz* contains a default configuration, and cannot be deleted.

Standard configurations

Devices without dual SIM functionality have a standard configuration (*Default-Configuration.tgz*) with which the configuration can be reset to the factory default settings. In the process, the access password and configurations stored in the device are retained. However, please note that the local IP address is also reset and the device can only be reached through the IP address 192.168.1.1 after the activation of a standard configuration.

ONLY PRODUCT VERSION DS

Devices of the product version DS have two standard configurations, one for each SIM card slot. These are identified with *Default-Configuration-SIM-1.tgz* and *Default-Configuration-SIM-2.tgz*. They have the same function as *Default-Configuration.tgz* in devices with only one SIM card and, like this standard configuration, cannot be deleted:



Loading and activating configuration profiles via SSH

Configuration profiles can also be loaded to the TAINY xMOD and activated with the SSH access (see chapter 9.4).

To do this, copy the configuration profile (e.g. TAINY.tgz) via SSH to the directory /webserver/profiles/.

Then copy a trigger file with the following name to the same directory:

<Configuration-profile>@now.trigger

As soon as the TAINY xMOD recognises this file in the directory, the new configuration profile is adopted. It makes no difference what the contents of the trigger file are.

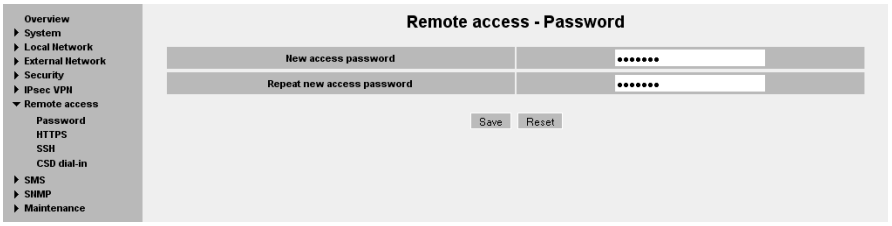
Example:

Configuration profile: TAINY.tgz

Trigger file: TAINY.tgz@now.trigger

3.9 Changing the password

Access > Authentication > Password



Function

Access to the TAINY xMOD is protected by an access password. This access password protects access by way of both the

- local interface to the Web user interface, and
- local interface to the SSH console,

as well as the access to the available wireless connection (HSPA+, UMTS, EGPRS or GPRS)

- by https to the web user interface, and
- by ssh to the SSH console

Access password (factory setting)

The factory setting for the TAINY xMOD is:

- Password: *root*
- User name: *root (*cannot be changed)

Note

Please change the password immediately after initial start-up. The factory setting is general knowledge and does not provide sufficient protection.

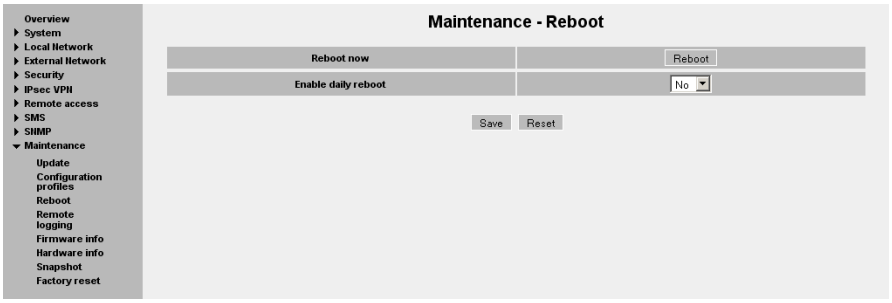
New access password (with confirmation)

To change the password, enter the new password you have selected in *New access password* and confirm the entry in *Repeat new access password.*

Reset can be used to discard any entries that have not yet been saved. *Save* accepts the new password.

3.10 Reboot

Maintenance > Reboot



Function

Although the TAINY xMOD is designed for continuous operation, in such a complex system faults may occur, often triggered by external influences. A reboot can rectify these faults.

The reboot resets the functions of the TAINY xMOD. Current settings according to the configuration profile do not change. The TAINY xMOD continues to work using these settings after the reboot.

Reboot now

The reboot is carried out immediately when you click on *Reboot*.

Enable daily reboot

The reboot is carried out automatically once a day if you switch the function on with *Yes*.

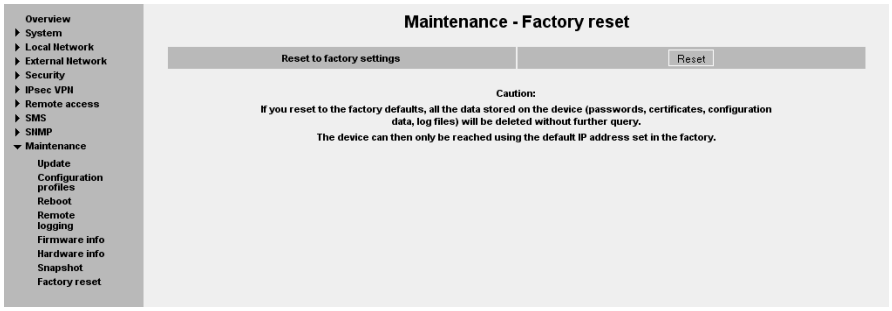
Specify the *Time of the daily reboot*. The reboot will be carried out at the specified system time. Existing connections will be interrupted.

Factory setting

Enable daily reboot:	**No**
Reboot time	**01:00**

3.11 Load factory settings

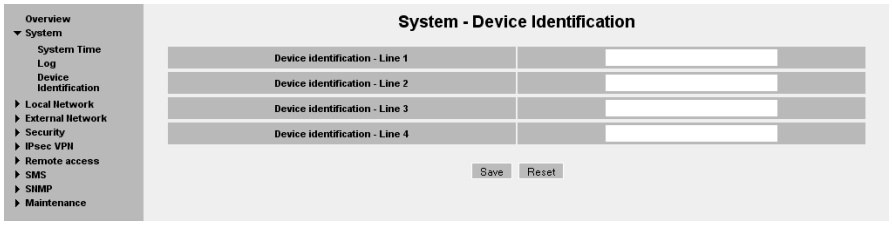
Maintenance > Factory Reset



Reset to factory settings	A click on the push button *Reset* loads the factory settings, resets the passwords and deletes the stored certificates, the configuration profiles and the archived log files. The TAINY xMOD-V3 will also delete the saved certificate.
Service button	The load of the factory settings can also be activated by pushing the service button (see chapter 2.5).
Default configuration	If you only intend to load the factory settings without deleting the configuration profiles and archived logs, then only activate the standard configuration as described in chapter 3.8.This process also applies to the certificates for the TAINY xMOD-V3.

3.12 Device identification

System > Device Identification

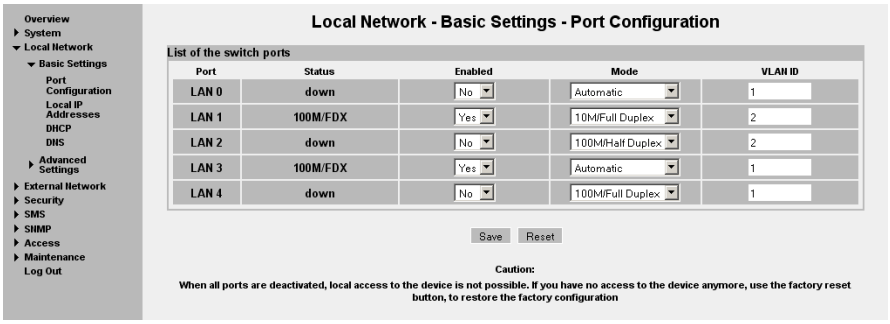


Device identification – Line 1 - 4	The TAINY xMOD provides four text fields in which the desired strings can be saved, for such purposes as device identification. The text fields can be written in and read. The text fields are each limited to 60 characters.
Character set	! $ % & ' ( ) * + , . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ _ ` a b c d e f g h I j k l m n o p q r s t u v w x y z { | }
SNMP	The four text fields can be read via SNMP (see chapter 12.1)

4 Local interface

4.1 Port Configuration

Local Network > Basic Settings > Port Configuration



Function

Each Ethernet port LANx of the TAINY xMOD can be activated and deactivated here separately. In addition you can determine the characteristics of the Ethernet LAN interfaces and you can combine interfaces to VLANs.

Status

Shows the current configuration of data rate and transmission mode of the interface:

Down	Interface not active
10M/HDX	Interface set to 10 Mbit / half duplex
10M/FDX	Interface set to 10 Mbit / full duplex
100M/HDX	Interface set to 100 Mbit / half duplex
100M/FDX	Interface set to 100 Mbit / full duplex

Enabled

Select *Yes* to enable the interface or *No* to disable it.

Mode

Used to configure the data rate and transmission mode of the interface:

Automatic	The configuration of the interface is negotiated automatically between both parties.
10M/HDX	Interface set to 10 Mbit / half duplex
10M/FDX	Interface set to 10 Mbit / full duplex
100M/HDX	Interface set to 100 Mbit / half duplex
100M/FDX	Interface set to 100 Mbit / full duplex

VLAN ID

The VLAN function (Virtual Local Area Network) facilitates to split the LAN interfaces of the TAINY xMOD-x3 into different, independent virtual networks. Local applications, which are connected to LAN interfaces with identical VLAN ID, can communicate via the TAINY xMOD-x3 among each other. If the VLAN IDs are different, a communication among each other is not possible.

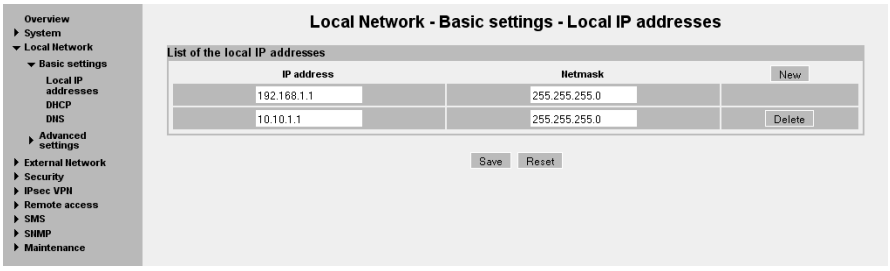
Factory settings

The factory settings for the TAINY xMOD are as follows:

Enabled	**Yes**
Mode	**Automatic**
VLAN ID	**1**

4.2 IP addresses of the local interface

Local Network > Basic Settings > Local IP Addresses

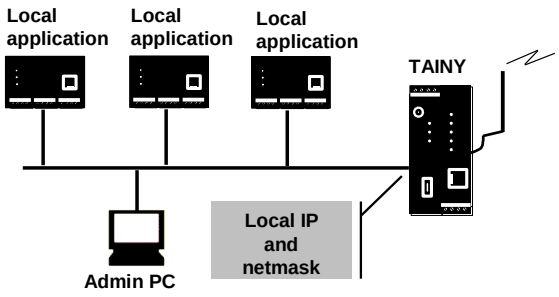


Local IP address acc. to factory setting: **192.168.1.1**

This is where the IP addresses and the net masks at which the TAINY xMOD can be reached by local applications are set. The factory settings for the TAINY xMOD are as follows:

IP	192.168.1.1
Netmask	255.255.255.0

These factory-set IP addresses and net masks can be changed freely, but should follow the applicable recommendations (RFC 1918).



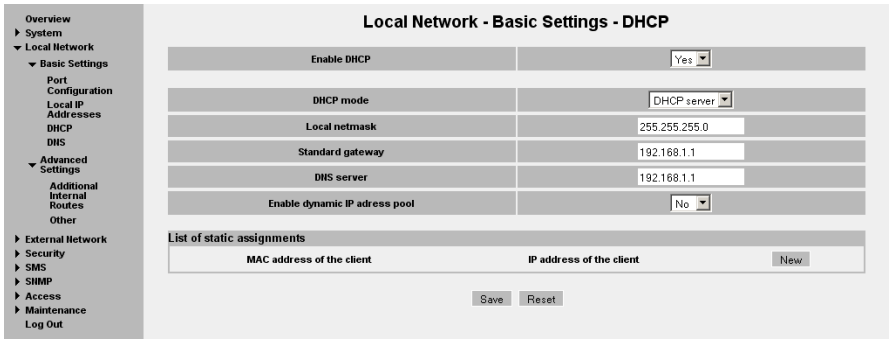
You can define additional addresses at which the TAINY xMOD can be reached by local applications. This is useful, for example, when the local network is subdivided into subnetworks. Then multiple local applications from different subnetworks can reach TAINY xMOD under various addresses.

New Adds additional IP addresses and net masks, which you can then modify in turn.

Delete Removes the respective IP address and netmask. The first entry cannot be deleted.

4.3 DHCP server to local network

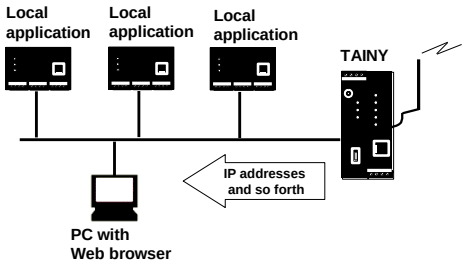
Local Network > Basic Settings > DHCP



DHCP function

The TAINY xMOD contains a DHCP server (DHCP = Dynamic Host Configuration Protocol). If the DHCP server is switched on and the DHCP server mode is selected, it automatically assigns to the applications that

are connected to the local interface of the TAINY xMOD the IP addresses, net masks, the gateway and the DNS server. This is only possible, if the setting for obtaining the IP address and the configuration parameters automatically via DHCP is activated for the local applications.



Alternatively the TAINY xMOD can also transfer DHCP requests coming from local applications via the WAN interface to a remote DHCP server, which answers the requests. Therefore you need to select the DHCP relay mode (see chapter 4.4).

Enable DHCP

Select *Enable DHCP* – *Yes* to activate the DHCP functions of the TAINY xMOD, select *No* to turn them off.

DHCP mode

Select *DHCP server* to activate the internal DHCP server of the TAINY xMOD. DHCP requests will be answered in this case directly by the TAINY xMOD.

Select *DHCP relay*, if the TAINY xMOD shall forward DHCP requests via the WAN interface to a remote DHCP server (see chapter 4.4).

Local netmask

Here enter the local netmask that should be assigned to the local applications.

Standard gateway

Here enter the default gateway that should be assigned to the local applications.

DNS server

Here enter the DNS server that should be assigned to the local applications.

Enable dynamic IP address pool

With *Yes* the IO addresses that the DHCP server of the TAINY xMOD assigns are drawn from a dynamic address pool.

With *No* the IP addresses must be assigned to the MAC addresses of the local application under *Static Leases*.

Range start

Specifies the first address of the dynamic address pool.

Range end

Specifies the last address of the dynamic address pool.

Static Leases

In Static Leases of the IP addresses you can assign corresponding IP addresses to the MAC addresses of local applications.

List of static assignments

If a local application requests assignment of an IP address via DHCP, the application communicates its MAC address with the DHCP query. If an IP address is statically assigned to this MAC address the TAINY xMOD assigns the corresponding IP address to the application. The assignment takes place through the *List of static assignments*.

MAC address of the client –

MAC address of the querying local application

IP address of the client –

assigned IP address

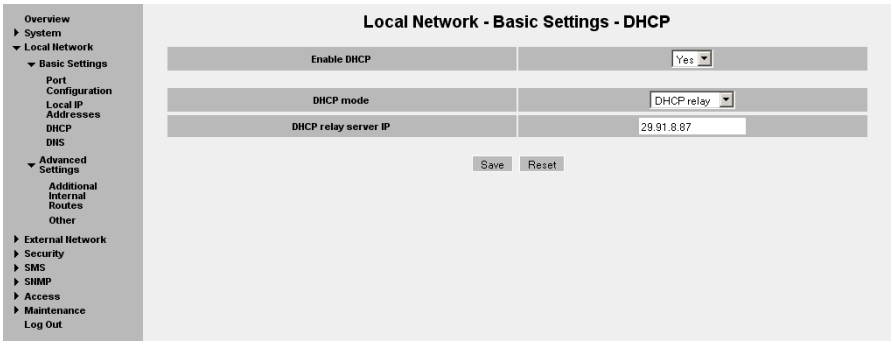
Factory setting

The factory settings for the TAINY xMOD are as follows:

Enable DHCP	**No**
DHCP mode	**DHCP server**
Local netmask	**255.255.255.0**
Standard gateway	**192.168.1.1**
DNS server	**192.168.1.1**
Enable dynamic IP address pool	**No**
Range start	**192.168.1.100**
Range end	**192.168.1.199**
MAC address of the client	**00:00:00:00:00:00**
IP address of the client	**0.0.0.0**

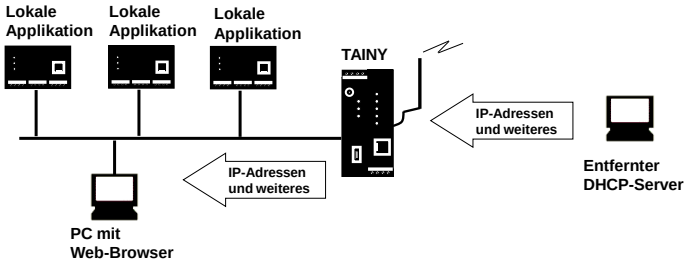
4.4 DHCP Relay to Local Network

Local Network > Basic Settings > DHCP



DHCP function

The TAINY xMOD is equipped with a DHCP relay function (DHCP = Dynamic Host Configuration Protocol). If the DHCP function of the TAINY xMOD is enabled and the DHCP relay mode is selected, the TAINY xMOD forwards DHCP requests coming from local applications via the WAN interface to a remote DHCP server, which answers the requests.



Alternatively the TAINY xMOD is equipped also with an internal DHCP server to reply to DHCP requests (see chapter 4.3).

Enable DHCP

Select *Enable DHCP – Yes* to activate the DHCP functions of the TAINY xMOD, select *No* to turn them off.

DHCP mode

Select *DHCP relay*, if the TAINY xMOD shall forward DHCP requests via the WAN interface to a remote DHCP server.

Select *DHCP server* to activate the internal DHCP server of the TAINY xMOD. DHCP requests will be answered in this case directly by the TAINY xMOD (see chapter 4.3).

DHCP relay server IP

Enter the IP address of the remote DHCP server.

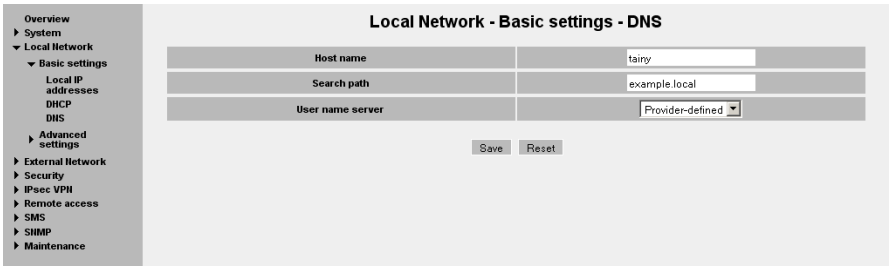
Factory setting

The factory settings for the TAINY xMOD are as follows:

Enable DHCP	**No**
DHCP mode	**DHCP server**
DHCP relay server IP	**0.0.0.0**

4.5 DNS to local network

Local Network > Basic Settings > DNS

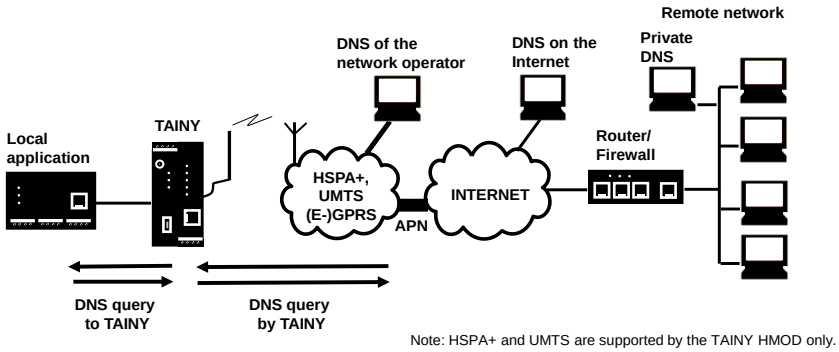


DNS function

The TAINY xMOD provides a domain name server (DNS) to the local network.

If you enter the IP address of the TAINY xMOD in your local application as the domain name server (DNS), then the TAINY xMOD answers the DNS queries from its cache. If it does not know the corresponding IP address for a domain address, then the TAINY xMOD forwards the query to an external domain name server (DNS).

The time period for which the TAINY xMOD holds a domain address in the cache depends on the host being addressed. In addition to the IP address, a DNS query to an external domain name server also supplies the life span of this information.



Note: HSPA+ and UMTS are supported by the TAINY HMOD only.

The external domain name server (DNS) used can be a server of the network operator, a server on the Internet, or a server in a private external network.

User name server

Select which domain name server (DNS) the TAINY xMOD should query.

Provider-defined	When a connection is established to UMTS/GPRS the network operator automatically communicates one or more DNS addresses. These are then used.
User-defined	As the user you select your preferred DNS. The DNSes can be connected to the Internet, or it can be a private DNS in your network.

User-defined name server

If you have selected the option *User-defined* then please enter the IP address of the selected DNS as the *Server IP Address*.

New can be used to add additional DNSes.

Factory setting

The factory settings for the TAINY xMOD are as follows:

User name server	**Provider-defined**
List of user-defined name servers	**-**
for new entry	**0.0.0.0**

4.6 Local host name

Local Network > Basic Settings > DNS

The TAINY xMOD can also be addressed from the local network using a host name. To do this, define a host name, e.g. *myTAINY*.

The TAINY xMOD can then be called up, for example from a Web browser as *myTAINY*.

Note

The security concept of the TAINY xMOD requires the creation of an outgoing firewall rule for each local application that is to use this host name function. See Chapter 6.1.

If you do not use DHCP (see Chapter 4.3), then identical search paths have to be entered manually in the TAINY xMOD and in the local applications. If you do use DHCP, the local applications received the search path entered in the TAINY xMOD via DHCP.

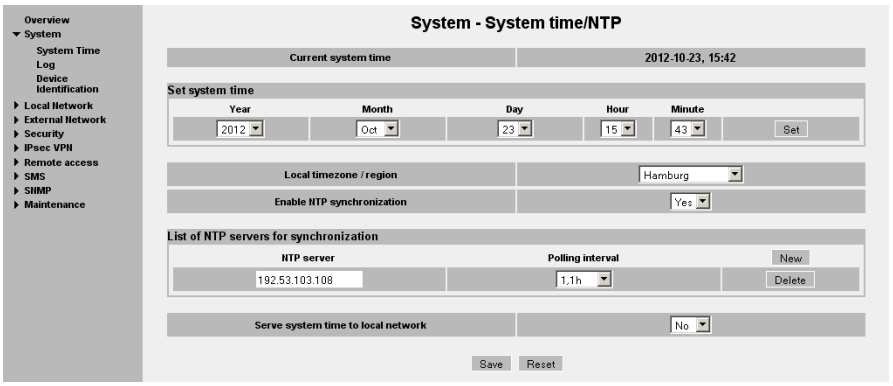
Factory setting

The factory settings for the TAINY xMOD are as follows:

Host name	**tainy**
Search path	**example.local**

4.7 System Time/NTP

System > System Time



Set system time

This is where you set the system time for the TAINY xMOD. This system time is:

- used as a time stamp for all log entries, and
- serves as a time basis for all time-controlled functions.

Select the year, month, day, hour and minute.

Enable NTP synchronization

The TAINY xMOD can also obtain the system time from a time server via NTP (= *Network Time Protocol*). There are a number of time servers on the Internet that can be used to obtain the current time very precisely via NTP.

Local time zone / region

The NTP time servers communicate the UTC (= *Universal Time Coordinated*). To specify the time zone, select a city near the location near where the TAINY xMOD will be operating. The time in this time zone will then be used as the system time.

NTP server

Click on *New* to add an NTP server, and enter the IP address of such an NTP server, or use the NTP server factory preset. You can specify multiple NTP servers at the same time.

It is not possible to enter the NTP address as a host name (e.g. timeserver.org).

Delete removes an NTP server from the *List of NTP servers for synchronization.*

Polling interval

The time synchronization is carried out cyclically. The interval at which synchronization is performed is determined by the TAINY xMOD automatically. A new synchronisation will be carried out at least once every 36 hours. The poll interval defines the minimum period that the TAINY xMOD waits until the next synchronization.

Note

Synchronising the system time via NTP causes additional data traffic on the wireless data connection. Depending on the selected settings, the additional data traffic can amount to 120 Kbytes per month or more. This entails higher costs, depending on the participant contract with the GSM network operator.

Serve system time to local network

The TAINY xMOD can serve itself as an NTP time server for the applications that are connected to its local network interface. To activate this function select *Yes*.

The NTP time server in the TAINY xMOD can be reached via the local IP address set for the TAINY xMOD, see Chapter 4.1.

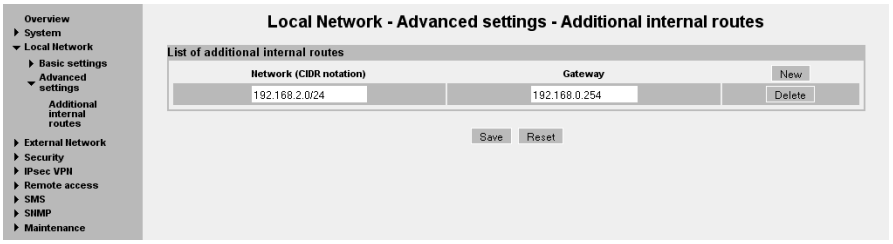
Factory setting

The factory settings for the TAINY xMOD are as follows:

Local time zone / region	**UTC**
Enable NTP synchronization	**No**
NTP server	**192.53.103.108**
Polling interval	**1.1 hours**
Serve system time to local network	**No**

4.8 Additional internal routes

Local Network > Advanced Settings > Additional Internal Routes



Function

If the local network is subdivided into subnetworks, you can define additional routes.

See also Chapter 16.

To define an additional route to a subnetwork, click on *New*.

Specify the following:

- the IP address of the subnetwork (*Network*), and also
- the IP address of the *Gateway* via which the subnet is connected.

You can define any desired number of internal routes.

To delete an internal route, click on *Delete*.

Factory setting

The factory settings for the TAINY xMOD are as follows:

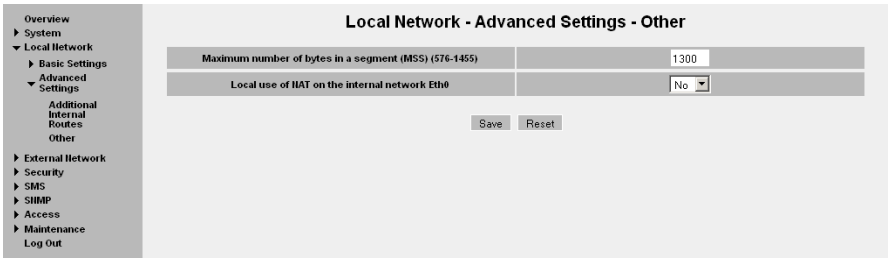
Additional Internal Routes	**-**

Default for new routes:

Network (CIDR notation)	**192.168.2.0/24**
Gateway	**192.168.0.254**

4.9 Advanced Settings for the Local Network

Local Network > Advanced Settings > Other



Function

This submenu contains advanced settings for the data handling in the local network.

Maximum number of bytes in a segment (MSS)

The Maximum Segment Size (MSS) determines the maximum number of Bytes the payload of a TCP segment may contain.

The value range for the parameter is 576 to 1455.

Local use of NAT on the internal network

With local NAT (Network Address Translation) on the internal network the source address of all data packages which are routed from the external WAN interface to the internal network by the TAINY xMOD will be replaced by the local IP address of the TAINY xMOD. This substitution may be important for specific applications.

Select *Yes* in order to use NAT locally on the internal network.

Select *No* in order to deactivate local use of NAT on the internal network.

Factory settings

The factory settings for the TAINY xMOD are as follows:

Maximum number of bytes in a segment	**1300**
Local use of NAT on the internal network	**No**

5 External interface

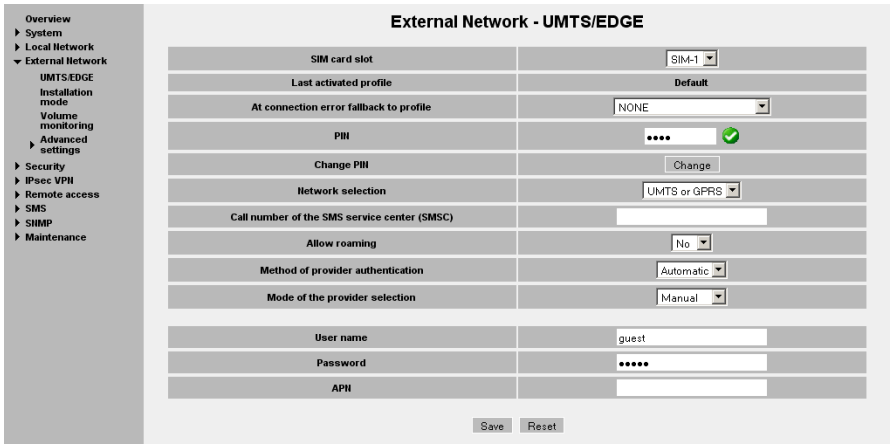
5.1 Network selection and access parameters for UMTS/GPRS

External Network > UMTS/EDGE

ONLY TAINY HMOD

External Network > EDGE/GPRS

ONLY TAINY EMOD

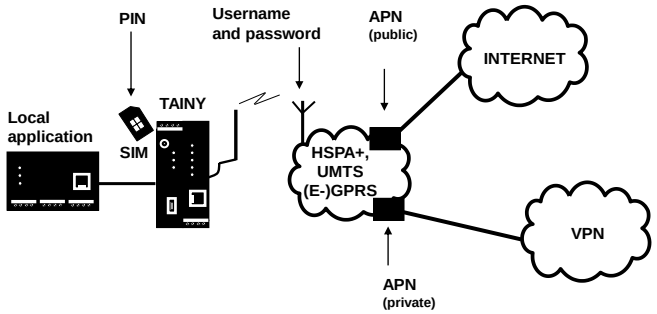


Function

The TAINY HMOD uses HSPA+, UMTS data, EGPRS or GPRS as the mobile data service for communication with the external network. The type of mobile communications network (UMTS or GSM) must be selected.

The TAINY EMOD uses EGPRS or GPRS as a mobile data service. Access parameters which you receive from your wireless network operator are required for access to these IP wireless network services and to the basic wireless network.

The PIN protects the SIM card against unauthorised use. The user name and password protect the access to the mobile radio services and the APN (Access Point Name) defines the transition from the mobile radio services to additional connected IP networks, for example a public APN to the Internet or a private APN to a virtual private network (VPN).



Note: HSPA+ and UMTS are supported by the TAINY HMOD only.

SIM card slot

ONLY PRODUCT VERSION DS

Select the SIM card slot to be used by the TAINY xMOD version DS (Dual SIM) when the current configuration is active here.

For more information about product version DS see chapter 14

Last activated profile

Displays the name of the latest activated configuration profile.

If no profile has been activated since bringing the TAINY xMOD into service or if the device has been reset to factory settings (see chapter 3.11) the display reads *Default*.

At connection error fallback to profile

Select the configuration profile from the profiles stored in the TAINY xMOD that will be activated if the device cannot establish a connection to the wireless data service (HSPA+, UMTS, EGPRS or GPRS) here. The

device will try to reconnect using the fallback profile.

If *NONE* is selected the fallback function is disabled (see chapter 15)

PIN

Enter the PIN for your SIM card here. You will receive the PIN from your network operator.

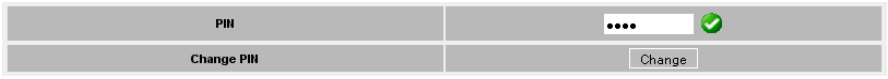
The TAINY xMOD also works with SIM cards that have no PIN; in this case please enter ***NONE***. In this case the input box is left empty.

Note

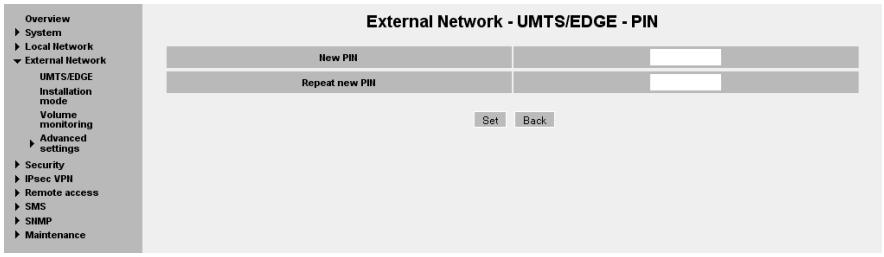
If no entry is made, the input box for the PIN is shown with a red outline after saving.

Change PIN

Press the *Change* button to change the PIN on the SIM card.



A submenu opens.



New PIN

Enter the new PIN here.

Repeat new PIN

Enter the new PIN again to confirm.

Note

If the PIN query is deactivated with the SIM card inserted (PIN-less card), then the PIN cannot be activated or changed.

Network selection

ONLY TAINY HMOD

The TAINY HMOD can be connected to the UMTS or GSM mobile communications networks at your discretion.

- UMTS (with the services UMTS data and HSPA+)
- GSM (with the services EGPRS, GPRS and CSD

With the setting *UMTS or GSM*, the TAINY HMOD preferentially selects a UMTS network depending on availability. If this is unavailable, a GSM network will be used.

With the setting *UMTS only*, the TAINY HMOD selects a UMTS network in any case.

With the setting *GSM only*, the TAINY HMOD selects a GSM network in any case.

Use antenna diversity

ONLY TAINY HMOD

To improve the wireless **reception quality**, an additional antenna can be connected (antenna diversity)

No — Select *No* in order to deactivate the antenna diversity function.

Yes — Select *Yes* in order to activate the antenna diversity function.

Call number of the SMS service center (SMSC)

The TAINY xMOD uses the Short Message Service (SMS) of GSM. It is possible to define a certain SMS Center

So that the SMS function will work reliably, enter the call number of the service center here. Without any entry the default SMS service center of your network operator will be used.

Attention:

It is strongly recommended to enter a call number for the SMS center and use the international format (e.g. +49...) to ensure the SMS can be sent. Otherwise you may encounter problems.

Allow roaming

The TAINY xMOD supports the following roaming modes:

No Select *No* if the TAINY xMOD should exclusively be logged into the home network (mobile communications network) whose SIM card is inserted.

Yes Select *Yes* if the TAINY xMOD may also be logged into partner networks of the home network if the home network cannot be reached or only with poor connectivity.

User In the *User* mode, the user defines a network ID using the parameter *Determine the location area identity (MCC/MNC)*, where the TAINY xMOD can book itself exclusively in the network. Other available wireless networks, including the home network of the SIM card, are ignored by the TAINY xMOD in this mode.

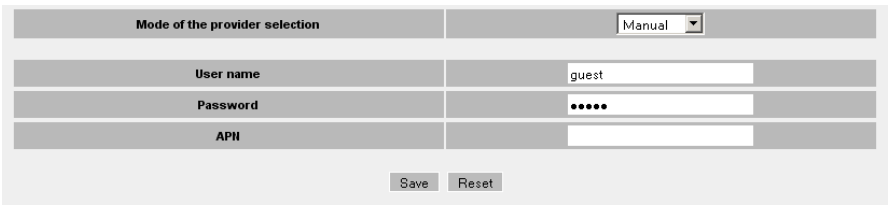
Warning

Considerable additional costs may be incurred if the TAINY xMOD logs into a partner network (roaming).

Method of provider authentication

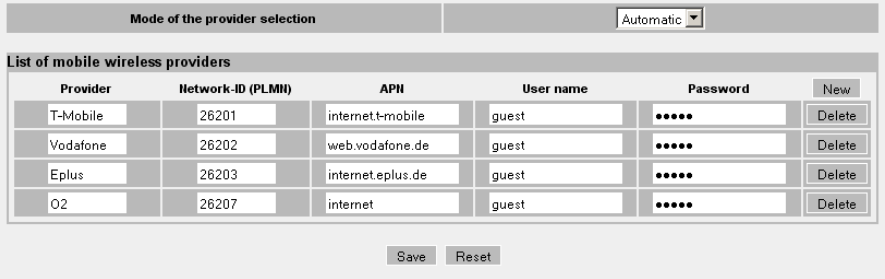
For registration at the wireless data service (HSPA+, UMTS, EGPRS or GPRS), two different methods (PAP and CHAP) are used. In general, the selection of the method is performed automatically. If a particular method shall be used, the selection may be done manually. Choose from Auto, PAP or CHAP.

Mode of the provider selection - Manual



If the Provider selection mode Manual is active, enter the User name, the Password and the APN for UMTS, EGPRS or GPRS manually.

Mode of the provider selection - Automatic



If the Provider selection mode Automatic is active, the access data for UMTS, EGPRS or GPRS are selected automatically. The access data will be selected depending on the Net-ID of the SIM carder from the provider list. Several entries can be inserted in the provider list. The quantity is not limited, but more than 10 entries should be avoided.

Click on New to insert a new entry. Click on Delete to remove entries.

Provider (only in case of provider selection mode Automatic)

Enter as free text the description of the UMTS or GPRS service, e.g. the Provider name (e.g. Vodafone, Eplus, my GPRS access).

Network-ID (PLMN) (only in case of provider selection mode Automatic)

Enter the identification number of the network provider to which the UMTS or GPRS access data of the same line of the provider list are related to.

Each UMTS or GSM/GPRS network has a worldwide unique identification number. This number is stored on the SIM card. The TAINY xMOD reads this Net-ID from the SIM card and selects the corresponding GPRS access data from the provider list.

You find the NET-ID at our website www.neuhaus.de, in the information documents of your UMTS or GSM/GPRS provider, at his homepage or you can ask the hotline of the provider (keyword: MCC/MNC).

APN

Enter the name of the transition from your wireless data service (HSPA+, UMTS, EGPRS or GPRS) to other networks here (for TAINY HMOD up to 100 characters, for TAINY EMOD up to 30 characters).

You can find the APN in your mobile radio network operator's documentation, on your operator's Website, or ask your operator's hotline.

User name

Enter the user name for your wireless data service (HSPA+, UMTS, EGPRS or GPRS) here (up to 127 characters). Some mobile radio network operators do not use access control with user names and/or passwords. In this case enter *guest* in the corresponding box.

Password

Enter the password for your wireless data service (HSPA+, UMTS, EGPRS or GPRS) here (up to 127 characters). Some mobile radio network operators do not use access control with user names and/or passwords. In this case enter *guest* in the corresponding box.

Factory setting

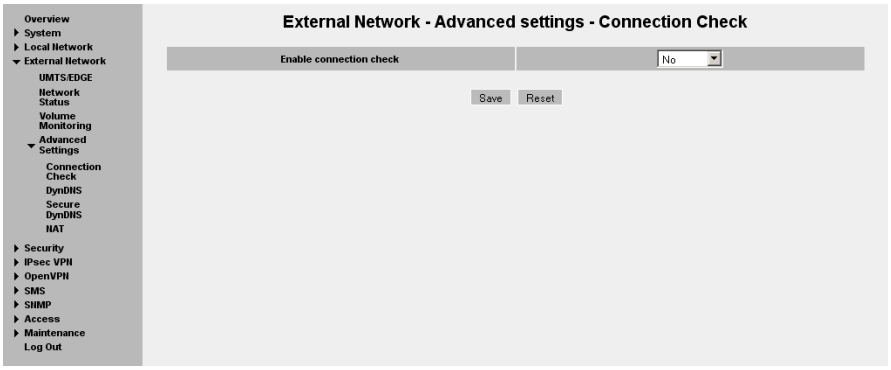
The factory settings for the TAINY xMOD are as follows:

ONLY PRODUCT VERSION DS	SIM card slot	**SIM-1**
	Last activated profile	**Default**
	At connection error fallback to profile	**NONE**
	PIN	**(empty)**
ONLY TAINY HMOD	Network selection	**UMTS or GSM**
ONLY TAINY HMOD	Use antenna diversity	**No**
	Call number of the SMS service center	**(empty)**

	Allow Roaming	**No**
	Method of provider authentication	**Automatic**
	Mode of the provider selection	**Automatic**
Mode of the provider selection - Manual	User name	**guest**
	Password	**guest**
	APN	**(empty)**
Mode of the provider selection - Automatic	1. Provider	**T-Mobile**
	Network-ID (PLMN)	**26201**
	User name	**guest**
	Password	**guest**
	APN	**internet.t-mobile**
	2. Provider	**Vodafone**
	Network-ID (PLMN)	**26202**
	User name	**guest**
	Password	**guest**
	APN	**web.vodafone.de**
	3. Provider	**Eplus**
	Network-ID (PLMN)	**26203**
	User name	**guest**
	Password	**guest**
	APN	**internet.eplus.de**
	4. Provider	**O2**
	Network-ID (PLMN)	**26207**
	User name	**guest**
	Password	**guest**
	APN	**internet**
	n. Provider	**NONE**
	Network-ID (PLMN)	**NONE**
	User name	**NONE**
	Password	**NONE**
	APN	**NONE**

5.2 UMTS/GPRS connection monitoring

External Network > Advanced Settings > Connection Check



Function

With the function *Connection Check* the TAINY xMOD checks its connection to UMTS/GPRS and to the connected external networks, such as the internet or an intranet. To do this, the TAINY xMOD sends ping packets (ICMP) to up to four remote stations (target hosts) at regular intervals.

The TAINY xMOD supports the following modes:

List — The TAINY xMOD sends ping packets to up to four remote locations (target hosts). If the TAINY xMOD receives an answer from at least one of the addressed remote locations, the TAINY xMOD is still connected to the mobile data service (HSPA+, UMTS, EGPRS or GPRS) and ready for operation (see chapter 0).

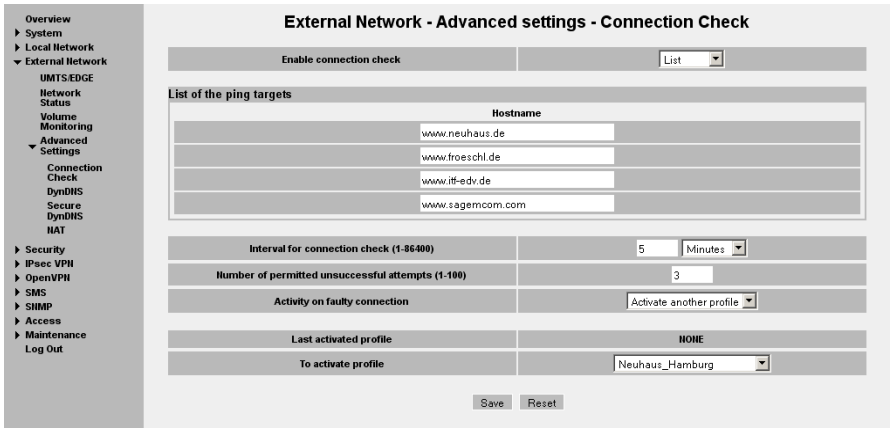
Statistics — The TAINY xMOD cyclically sends a variable number of ping packets (*burst*) to exactly one target host and observes the answer behaviour over a specific period of time. If a specified quota of answers (*success threshold*) is received over this observation period, the test has been passed and the device is still connected to the mobile data service (see chapter 5.2.2).

The transmission of ping packets takes place independently of the user data connections.

Some network operators interrupt connections when they are inactive. This is likewise prevented by the *Connection Check* function.

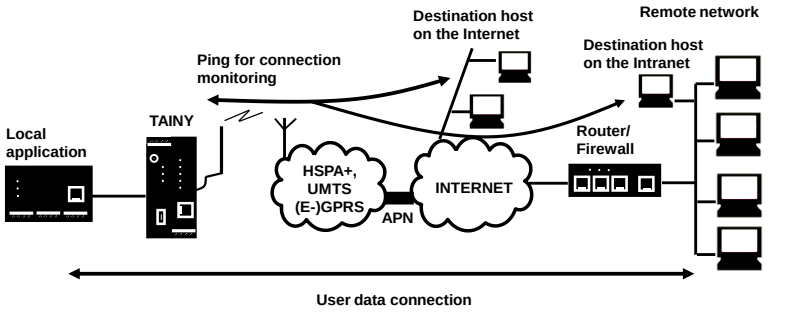
5.2.1 “List“ Mode

External Network > Advanced Settings > Connection Check



Function

In *List* mode the TAINY xMOD sends ping packets (ICMP) in regular intervals to up to four remote locations (target hosts). This takes place independently of the usage data connections. If the TAINY xMOD receives an answer to one such ping from at least one of the addressed remote locations, the TAINY xMOD is still connected to the mobile data service (HSPA+, UMTS, EGPRS or GPRS) and ready for operation.



Note: HSPA+ and UMTS are supported by the TAINY HMOD only.

Warning

Sending ping packets (ICMP) increases the amount of data sent and received via the UMTS/GPRS. The additional data traffic can add up to 2.5 Mbyte per month (ping to IP address) or 6 Mbyte per month (ping to host name), depending on the settings selected. This can lead to increased costs.

Enable connection check

List activates the function in *List* mode.

List of the ping targets - Host name

Select up to four remote stations that the TAINY xMOD can ping. The remote stations must be available continuously and must answer pings.

Note

Make sure that the selected remote stations will not feel "harassed".

Interval for connection check

Specifies the interval at which the connection check ping packets are sent by the TAINY xMOD. The entered value is specified as a minute or second value via the drop down menu.

Number of permitted unsuccessful attempts

Specifies how many times it is allowed for all ping packets of an interval not to receive an answer, i.e. for none of four pinged remote stations to answer, before the specified action is carried out.

Activity on faulty connection

Renew connection — The TAINY xMOD re-establishes the connection to the UMTS/GPRS if the ping packets sent were not answered.

Restart the device	The TAINY xMOD performs a reboot if the ping packets sent were not answered.
Activate another profile	The TAINY xMOD activates a substitute profile and tries to reconnect to the wireless data service (HSPA+, UMTS, EGPRS or GPRS) if the ping packets sent were not answered. Once the option *Activate another profile* has been selected, a dialog to specify a substitute profile opens.

Last activated profile	Displays the name of the latest activated configuration profile.
To activate profile	Select the configuration profile from the profiles stored in the TAINY xMOD that will be activated if the connection check fails here.

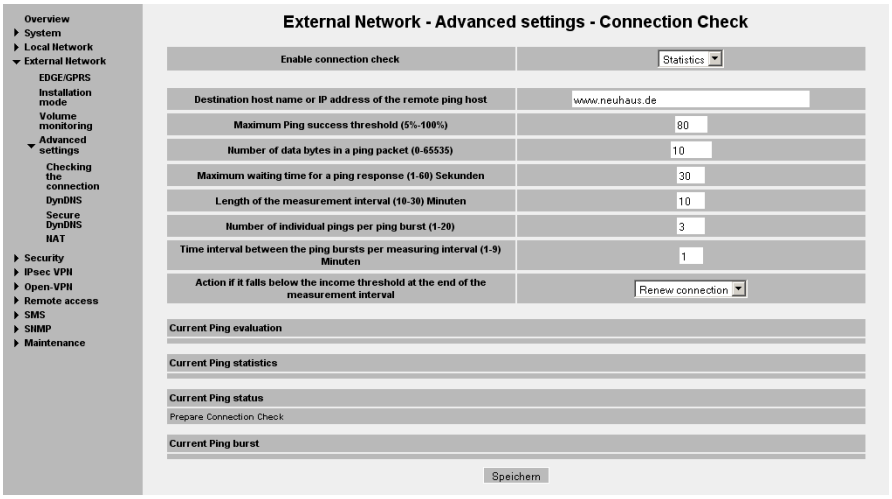
Factory setting

The factory settings for the TAINY xMOD are as follows:

Enable connection check	**No (switched off)**
Host name	**-**
Interval for connection check (minutes)	**5 (minutes)**
Number of permitted unsuccessful attempts	**3 (failed attempts)**
Activity on faulty connection	**Renew Connection**
To activate profile	**NONE**

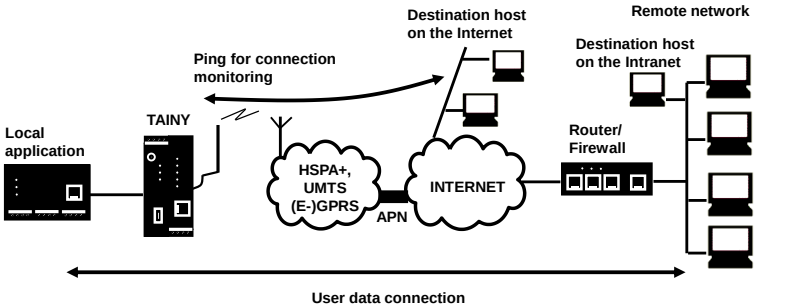
5.2.2 "Statistics" Mode

External Network > Advanced Settings > Connection Check



Function

In *Statistics* mode the TAINY xMOD sends ping *bursts* to exactly one remote location (target host) in regular intervals. "Burst" refers to the sending of one ping packet or multiple ping packets in immediate succession.



Note: HSPA+ and UMTS are supported by the TAINY HMOD only.

The answer behaviour of the remote location - unlike in *List* mode - is observed over a variable period of time, the *measurement interval*.

In the process, after the lapse of the measurement interval the TAINY xMOD calculates the number of all ping answers received within the measurement interval in relation to the number of ping packets sent.

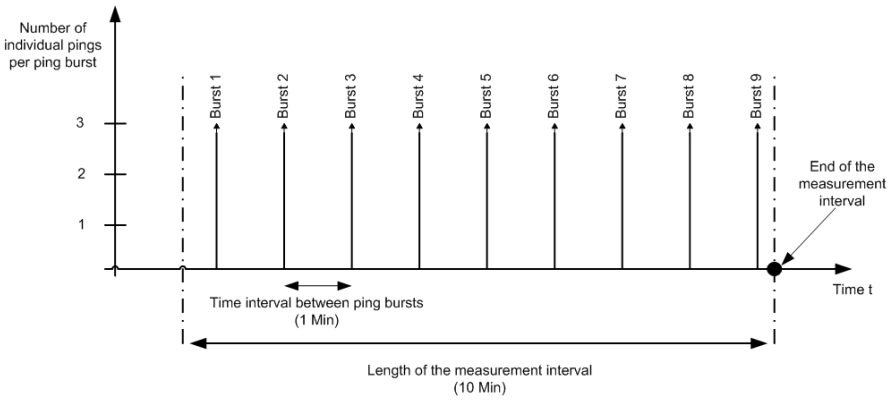
The result of this calculation is compared with the variable *success threshold*. If this threshold is reached or exceeded, the TAINY xMOD applies as still connected to the mobile data service (HSPA+, UMTS, EGPRS or GPRS) and ready for operation.

The statistical evaluation, which is supplemented with entries in a log, additionally provides information about the quality of an existing connection.

The connection test is performed independently of existing usage data connections.

Time response

The following graph provides an overview of the time response of the TAINY xMOD in *Statistics* mode. In this example the measurement interval is 10 min; bursts of three ping commands each are sent one minute apart.

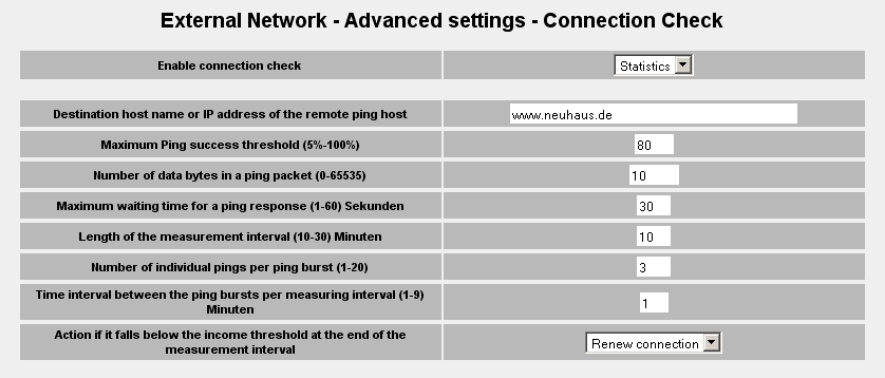


Warning

By sending the ping packets (ICMP), the amount of data sent and received over the mobile data service connection (HSPA+, UMTS, EGPRS or GPRS) increases. Depending on the selected settings (time response, number of ping commands per burst, length of the ping packets, etc.), the additional data traffic can amount to several Mbyte per month.

This can lead to additional costs.

Parameterization



Enable connection check

Statistics enables the *Statistics* mode.

Destination host name or IP address of the remote ping host

Specify the host name of the IP address of the remote location to which the TAINY xMOD should send ping commands in the scope of the connection test. The remote location must be available at all times and respond to the ping packets.

Note

Make sure that the selected remote location does not feel "stressed" by the ping packets.

Ping success threshold

Here you specify the threshold for successful ping tests which must be reached or exceeded at the end of the measurement interval so that the TAINY xMOD can be connected to the WAN and declared ready for operation.

The value range for the parameter is 5 % to 100 %.

Number of data bytes in a ping packet

Here you specify the length in bytes of the ping packets which should be sent for the testing of the connection.

The value range for the parameter is 0 to 65535.

Maximum waiting time for a ping response

Here you specify the time in seconds within which an answer to a sent ping packet must reach the TAINY xMOD so that this ping packet can be assessed as successfully answered.

The value range for the parameter is 1 s to 60 s.

Length of the measurement interval

Defines the length of the measurement interval in minutes.

The value range for the parameter is 10 min to 30 min.

Number of individual pings per ping burst

Ping bursts are sent in a variable interval in *Statistics* mode. Here you specify how many ping packets should be sent per burst.

The value range for the parameter is 1 to 20.

Time interval between the ping bursts

Here you specify the time interval in which bursts should take place.

The value range for the parameter is 1 min to 9 min.

Action if it falls below the income threshold at the end of the measurement interval

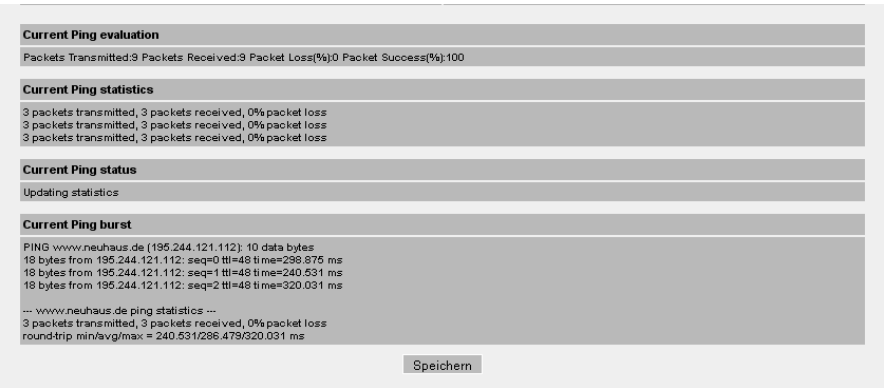
Renew connection	The TAINY xMOD re-establishes the connection to the UMTS/GPRS, if the ping success threshold has not been reached at the end of the measurement interval.
Restart the device	The TAINY xMOD performs a reboot, if the ping success threshold has not been reached at the end of the measurement interval.
Activate profile	The TAINY xMOD activates a substitute profile and tries to reconnect to the wireless data service

(HSPA+, UMTS, EGPRS or GPRS), if the ping success threshold has not been reached at the end of the measurement interval.

Once the option *Activate profile* has been selected, a dialog to specify a substitute profile opens.

Last activated profile	Displays the name of the latest activated configuration profile.
To activate profile	Select the configuration profile from the profiles stored in the TAINY xMOD that will be activated if the connection check fails here.

Statistics



In *Statistics* mode the website provides various statistical values of the measurement interval currently in progress. The example above shows the data of a connection test after three bursts of three ping commands each. All ping commands were successfully answered.

After the lapse of the measurement interval the data is evaluated and the display is deleted.

Current Ping evaluation	Shows the evaluation of all ping tests performed thus far in the current measurement interval. The result calculated here (*packet success*) is compared with the *ping success threshold* at the end of the measurement interval.
Current Ping statistics	Lists the evaluation of all ping bursts performed thus far in the current measurement interval on an individual basis.
Current Ping status	Shows the current status of the ping test.
Current Ping Burst	Lists the evaluation of the ping commands sent in the last ping burst, including the packet circulation time.

Factory setting

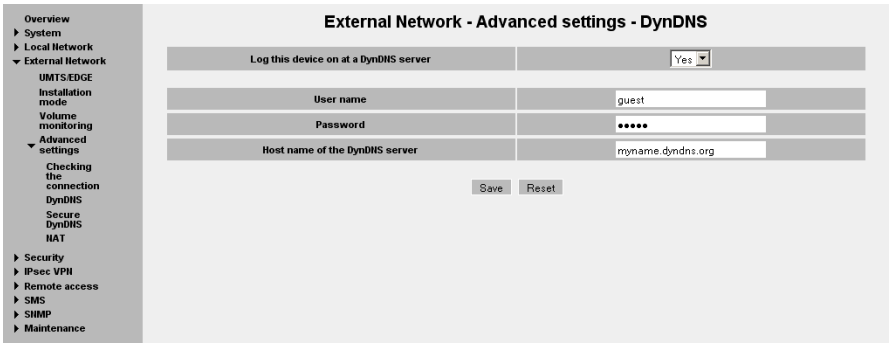
The factory settings for the TAINY xMOD are as follows:

Enable connection check	**No (disabled)**
Destination host name or IP address of the remote ping host	**NONE (empty)**
Ping success threshold	**80**
Number of data bytes in a ping packet	**10**
Maximum waiting time for a ping response	**30**
Length of the measurement interval	**10**
Number of individual pings per ping burst	**10**

Time interval between the ping bursts	**1**
Action if it falls below the income threshold at the end of the measurement interval	**Renew connection**
To activate profile	**NONE**

5.3 Host name via DynDNS

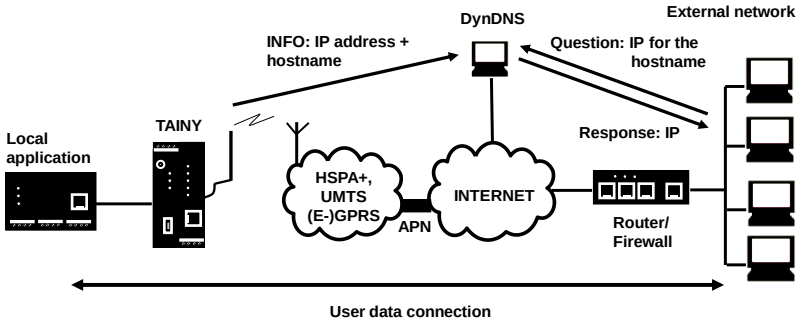
External Network > Advanced Settings > DynDNS



Function

Dynamic domain name servers (DynDNS) make it possible for applications to be accessible on the Internet under a host name (e.g. myHost.org), even if these applications do not have a fixed IP address and the host name is not registered. If you log the TAINY xMOD on to a DynDNS service, you also can reach the TAINY xMOD from external networks under a host name, e.g. myTainy.dyndns.org. The TAINY xMOD is compatible with **dyndns.org**.

For more information on DynDNS see Chapter 16.



Note: HSPA+ and UMTS are supported by the TAINY HMOD only.

Log this device on at a DynDNS server

Select *Yes* if you want to use a DynDNS service.

User name / Password

Enter here the user name and the password that authorise you to use the DynDNS service. Your DynDNS provider will give you this information.

Host name of the DynDNS server

Here enter the host name that you have agreed with your DynDNS provider for the TAINY xMOD, e.g. myTAINY.dyndns.org.

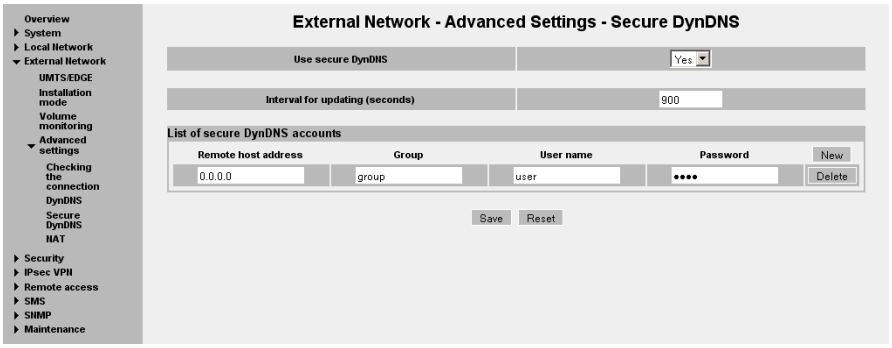
Factory setting

The factory settings for the TAINY xMOD are as follows:

Log this device on at a DynDNS server	**No (switched off)**
User name	**guest**
Password	**guest**
Host name of the DynDNS server	**myname.dyndns.org**

5.4 Secure DynDNS

External Network > Advanced Settings > Secure DynDNS



Function

With Secure DynDNS being activated, the TAINY xMOD transmits its external IP address being assigned by the EDGE/GPRS service via secured https protocol to a selectable remote host.

This function is comparable to DynDNS service and requires an applicable access point at the host side.

Use Secure DynDNS

Click *Yes*, if you like to use the Secure DynDNS.

Click *New* to add additional remote hosts, click *Delete* to remove existing entries.

Interval for updating (seconds)

Enter the interval in seconds, applied to transmit periodically the IP address of the TAINY xMOD to the remote host.

List of Secure DynDNS accounts

Enter the target IP address and the access data of one or more remote hosts.

Remote host address

Enter the target IP address of the remote host.

Group

Enter the group information.

User name

Enter the User name to access the remote host.

Password

Enter the Password to access the remote host.

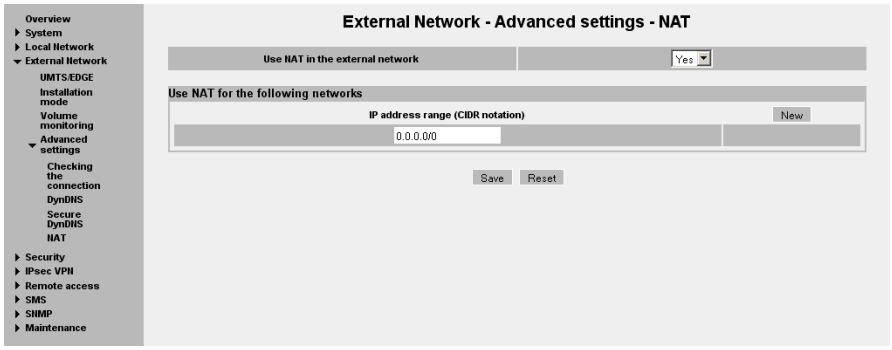
Factory setting

The factory settings for the TAINY xMOD are as follows:

Use Secure DynDNS	No (switched off)
Interval for updating (seconds)	900 seconds
Remote host address	0.0.0.0
Group	group
User name	user
Password	pass

5.5 NAT – Network address translation

External Network > Advanced Settings > NAT



Function

This lists the fixed rules for NAT (**N**etwork **A**ddress **T**ranslation) and allows rules to be set or deleted.

For outgoing data packets the TAINY xMOD can translate the given sender IP addresses from its internal network to its own external address, a technique known as NAT (Network Address Translation).

This method is used when the internal addresses cannot or should not be routed, e.g. because a private address range such as 192.168.x.x or the internal network structure is to be hidden.

This method is also called *IP Masquerading*.

Use NAT in the external network

Select *Yes* if you want to use the NAT function.

Use NAT for the following networks

Enter the network to which NAT shall be applied to. To denote a range, use CIDR syntax.

New – Add a network

Delete – Delete a network

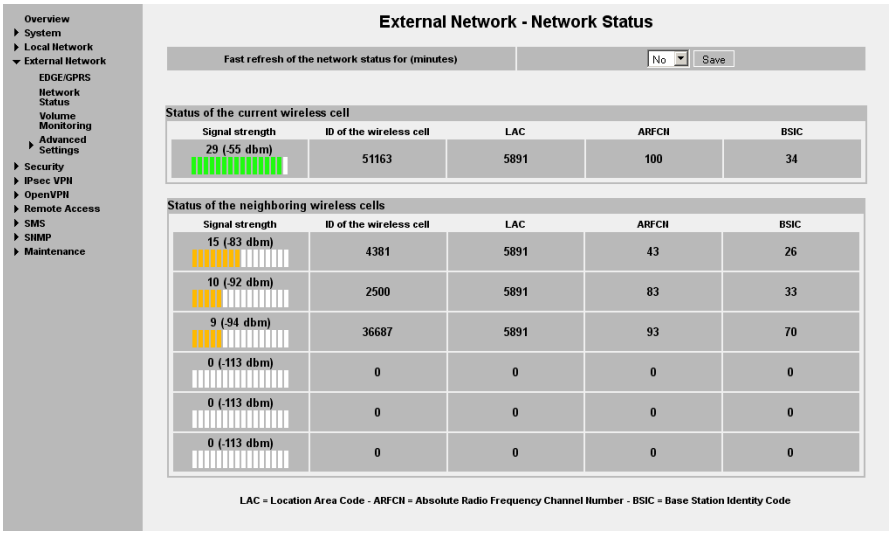
Factory setting

The factory settings for the TAINY xMOD are as follows:

Use NAT for the external network	**Yes (switched on)**
IP address range (CIDR notation)	**0.0.0.0/0**.

5.6 Network status

External Network > Network Status



The *Network status* page contains information on the wireless cell currently used and visible wireless cells in the vicinity of the TAINY xMOD.

In normal operation, the signal strengths and characteristics for the wireless cells shown in *Network status* are updated every 60 seconds. In order to support the positioning of the antenna(s), the *Fast refresh of the network status* mode can also be activated. In this mode, the TAINY xMOD updates the values shown here, as well as the display of the *Signal* LED Q (Quality) approximately every 3 seconds.

The position of the antenna(s) should be changed until the displayed signal of the current cell has reached a maximum.

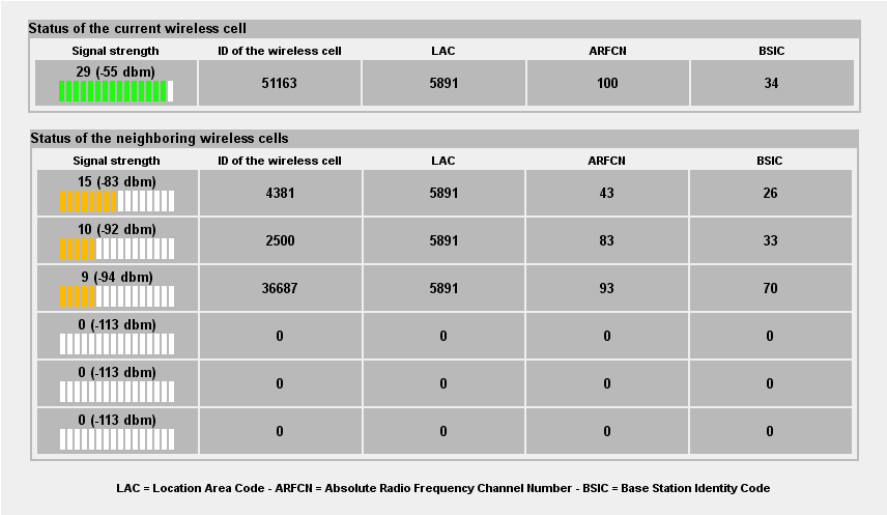
Regardless of the set mode, i.e. the status of the values, the website updates approximately every 3 seconds.

Fast refresh of the network status for (minutes)

To activate the *Fast refresh of the network status* mode, select one of the specified minute values and apply it with *Save*. Once the set time has elapsed, the *Fast refresh* is finished automatically and the device returns to normal operation.

Select *No* and click *Save* to switch off the *fast refresh of the network status* and return to normal operation.

5.6.1 Network status (2G) - TAINY EMOD



Status of the current wireless cell — Shows the characteristics of the cell to which the TAINY xMOD is currently connected.

Status of the neighboring wireless cell — Shows the characteristics of neighboring cells from which the TAINY xMOD receives signals.

Signal strength — Display of the quality/field strength with which the signal of the cell is received. The CSQ value is specified and converted as an RSSI value [dBm].

ID of the wireless cell — Specifies the identification (Cell ID) of the cell.

LAC — Specifies the identification (LAC) of the network section comprised of multiple base stations / cells in the vicinity of the TAINY xMOD.

ARFCN — Indicates the number (ARFCN) of the radio channel on which the cell broadcasts.

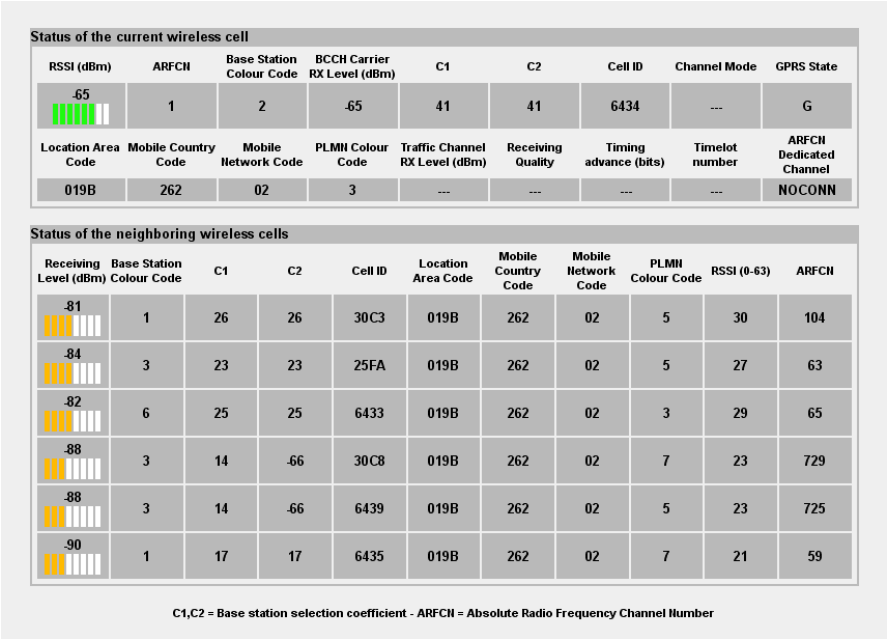
BSIC — Specifies the identification (BSIC) of the base station to which the cell belongs.

Factory setting

The factory settings for the TAINY xMOD are as follows:

Fast refresh of the network status (minutes)	**No (switched off)**

5.6.2 Network status (2G) - TAINY HMOD



Status of the current wireless cell

RSSI (dBm)	ARFCN	Base Station Colour Code	BCCH Carrier RX Level (dBm)	C1	C2	Cell ID	Channel Mode	GPRS State
-65	1	2	-65	41	41	6434	---	G

Location Area Code	Mobile Country Code	Mobile Network Code	PLMN Colour Code	Traffic Channel RX Level (dBm)	Receiving Quality	Timing advance (bits)	Timelot number	ARFCN Dedicated Channel
019B	262	02	3	---	---	---	---	NOCONN

Status of the neighboring wireless cells

Receiving Level (dBm)	Base Station Colour Code	C1	C2	Cell ID	Location Area Code	Mobile Country Code	Mobile Network Code	PLMN Colour Code	RSSI (0-63)	ARFCN
-81	1	26	26	30C3	019B	262	02	5	30	104
-84	3	23	23	25FA	019B	262	02	5	27	63
-82	6	25	25	6433	019B	262	02	3	29	65
-88	3	14	-66	30C8	019B	262	02	7	23	729
-88	3	14	-66	6439	019B	262	02	5	23	725
-90	1	17	17	6435	019B	262	02	7	21	59

C1,C2 = Base station selection coefficient - ARFCN = Absolute Radio Frequency Channel Number

Status of the current wireless cell	Shows the characteristics of the cell to which the TAINY xMOD is currently connected.
RSSI (dBm)	Indicates the overall power of the received signals on the currently used channel in dBm.
ARFCN	Indicates the **A**bsolute **R**adio **F**requency **C**hannel **N**umber of the BCCH (Broadcast Control Channel) carrier.
Base Station Colour Code	Shows the colour code of the base station.
BCCH Carrier RX Level (dBm)	Shows the receiving level of the BCCH (Broadcast Control Channel) carrier.
C1	Shows coefficient 1 for the base station selection.
C2	Shows coefficient 2 for the base station selection.
Cell ID	Specifies the identification of the wireless cell.
Channel Mode	Specifies which mode the dedicated channel is using.
GPRS State	Shows the state of the GPRS connection.
Location Area Code	Specifies the identification (LAC) of the network section comprised of multiple base stations / cells in the vicinity of the TAINY xMOD.
Mobile Country Code	Shows the country code (MCC) of the currently used wireless service provider.
Mobile Network Code	Shows the network code (MNC) of the currently used wireless service provider.
PLMN Colour Code	Shows the colour code of the wireless service provider serving the base station of the currently used cell.
Traffic Channel RX	Shows the receiving level of the traffic channel in dBm.

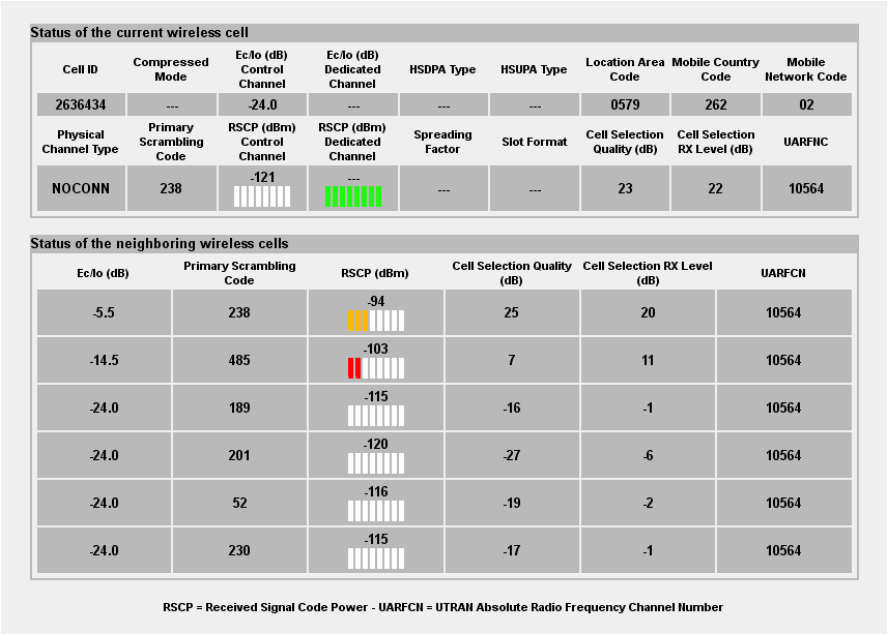
Level (dBm)	
Receiving Quality	Shows the receiving quality of the dedicated channel (0-7).
Timing advance (bits)	Shows the timing advance in bits (dedicated channel).
Timeslot number	Shows the currently used timeslot number (dedicated channel).
ARFCN Dedicated Channel	Indicates the absolute radio frequency number of the dedicated channel.
Status of the neighboring wireless cells	Shows the characteristics of neighboring wireless cells from which the TAINY xMOD receives signals.
Receiving Level (dBm)	Specifies the receiving level in dBm (neighboring cell).
Base Station Colour Code	Shows the colour code of the base station (neighboring cell).
C1	Shows coefficient 1 for the base station selection (neighboring cell).
C2	Shows coefficient 2 for the base station selection (neighboring cell).
Cell ID	Specifies the identification of the neighboring cell.
Location Area Code	Specifies the identification (LAC) of the network section comprised of multiple base stations / cells in the vicinity of the TAINY xMOD (neighboring cell).
Mobile Country Code	Shows the country code (MCC) of the wireless network provider (neighboring cell).
Mobile Network Code	Shows the network code (MNC) of the wireless network provider (neighboring cell).
PLMN Colour Code	Shows the colour code of the wireless network provider serving the base station of the neighboring cell.
RSSI (0-63)	Indicates the overall power of the received signal on the specific channel (neighboring cell).
ARFCN	Indicates the absolute radio frequency channel number of the BCCH (Broadcast Control Channel) carrier (neighboring cell).

Factory setting

The factory settings for the TAINY xMOD are as follows:

Fast refresh of the network status (minutes)	**No (switched off)**

5.6.3 Network status (3G)



Status of the current wireless cell

Cell ID	Compressed Mode	Ec/Io (dB) Control Channel	Ec/Io (dB) Dedicated Channel	HSDPA Type	HSUPA Type	Location Area Code	Mobile Country Code	Mobile Network Code
2636434	---	-24.0	---	---	---	0579	262	02

Physical Channel Type	Primary Scrambling Code	RSCP (dBm) Control Channel	RSCP (dBm) Dedicated Channel	Spreading Factor	Slot Format	Cell Selection Quality (dB)	Cell Selection RX Level (dB)	UARFNC
NOCONN	238	-121	---	---	---	23	22	10564

Status of the neighboring wireless cells

Ec/Io (dB)	Primary Scrambling Code	RSCP (dBm)	Cell Selection Quality (dB)	Cell Selection RX Level (dB)	UARFCN
-5.5	238	-94	25	20	10564
-14.5	485	-103	7	11	10564
-24.0	189	-115	-16	-1	10564
-24.0	201	-120	-27	-6	10564
-24.0	52	-116	-19	-2	10564
-24.0	230	-115	-17	-1	10564

RSCP = Received Signal Code Power - UARFCN = UTRAN Absolute Radio Frequency Channel Number

Status of the current wireless cell	Shows the characteristics of the cell to which the TAINY xMOD is currently connected.
Cell ID	Specifies the identification (Cell ID) of the cell.
Compressed Mode	Shows whether the device is working in Compressed Mode.
Ec/Io (dB) Control Channel	Shows the signal-to-noise ratio of the control channel.
Ec/Io (dB) Dedicated Channel	Shows the signal-to-noise ratio of the data channel.
HSDPA Type	Shows the **H**igh **S**peed **D**ownload **P**acket **A**ccess type. This parameter is not provided by all wireless service providers.
HSUPA Type	Shows the **H**igh **S**peed **U**pload **P**acket **A**ccess type. This parameter is not provided by all wireless service providers.
Location Area Code	Specifies the identification (LAC) of the network section comprised of multiple base stations / cells in the vicinity of the TAINY xMOD.
Mobile Country Code	Shows the country code (MCC) for the wireless service provider used.
Mobile Network Code	Shows the network code (MNC) for the wireless service provider used.
Physical Channel Type	Shows the type of the physical transmission channel.
Primary Scrambling Code	Shows the individual encryption code, which can be used to assign data packages clearly to the base station/wireless cell used.
RSCP (dBm) Control Channel	Shows the demodulated channel output of the control channel.
RSCP (dBm) Dedicated Channel	Shows the demodulated channel output of the data channel.
Spreading Factor	Shows the spreading factor for the data transmission via the UMTS network.
Slot Format	Shows the slot format of the physical transmission channel.
Cell Selection Quality (dB)	Shows the *Cell Selection Quality* value, which is used among other things for selecting the wireless cell to be used.

Cell Selection Rx Level (dB)	Shows the *Cell Selection Rx Level* value, which is used among other things for selecting the wireless cell to be used.
UARFCN	Indicates the absolute number of the radio channel on which the current cell broadcasts.
Status of the neighboring wireless cells	Shows the characteristics of neighboring wireless cells from which the TAINY xMOD receives signals.
Ec/Io (dB)	Shows the signal-to-noise ratio of the channel of the relevant neighboring cell.
Primary Scrambling Code	Shows the individual encryption code of the relevant neighboring cell.
RSCP (dBm)	Shows the demodulated channel output of the relevant neighboring cell.
Cell Selection Quality (dB)	Shows the *Cell Selection Quality* value of the relevant neighboring cell.
Cell Selection Rx Level (dB)	Shows the *Cell Selection Rx Level* value of the relevant neighboring cell.
UARFCN	Indicates the absolute number of the radio channel on which the neighboring cell broadcasts.

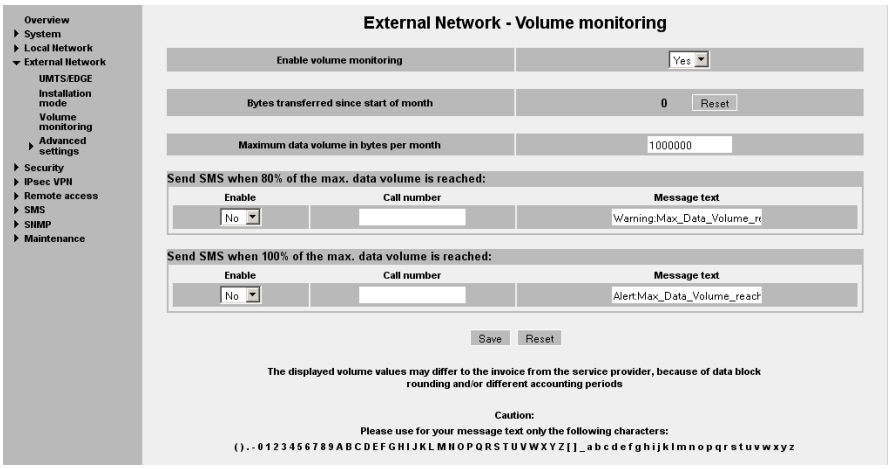
Factory setting

The factory settings for the TAINY xMOD are as follows:

Fast refresh of the network status (minutes)	**No (switched off)**

5.7 Volume monitoring

External Network > Volume Monitoring



Considerable additional costs may be incurred if the amount of data sent and received by the TAINY xMOD exceeds the data volume agreed upon with the wireless network operator.

Therefore, it may be beneficial if the data volume the TAINY xMOD uses is monitored and a warning is issued when a variable limit value is approached.

Note

The data volume detected only serves as an indication and may deviate from the calculation of the GSM network operator.

Enable volume monitoring	Select *Yes* in order to switch on the traffic volume supervision.

	Select *No* in order to switch off the traffic volume supervision.
Bytes transferred since start of month	Shows the number of bytes sent and received since the beginning of the month.
	Note Manually set the system time of the TAINY xMOD or activate the NTP synchronization, see chapter 4.7.
Reset	Press the button if you want to reset the counter for the bytes sent and received to 0. This takes place automatically at the end of the month.
Maximum data volume in bytes per month	Enter the limit value for the monthly data volume in bytes here.
Send SMS when 80% of the max. data volume is reached	Set *Enable* to *Yes* if you want the TAINY xMOD to send an SMS with a warning message to the specified call number upon reaching 80% of the maximum data volume.
Send SMS when 100% of the max. data volume is reached	Set *Enable* to *Yes* if you want the TAINY xMOD to send an SMS with an alert message to the specified call number upon reaching the maximum data volume.
Call number	Enter the mobile call number which the SMS with the alarm or warning message should be sent to here.
Text	Enter the text of the alarm or warning SMS here.
Character set	The following characters are supported: , * ' # % = <> ! & + - / ? ( ) . : ; 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z (and Space)

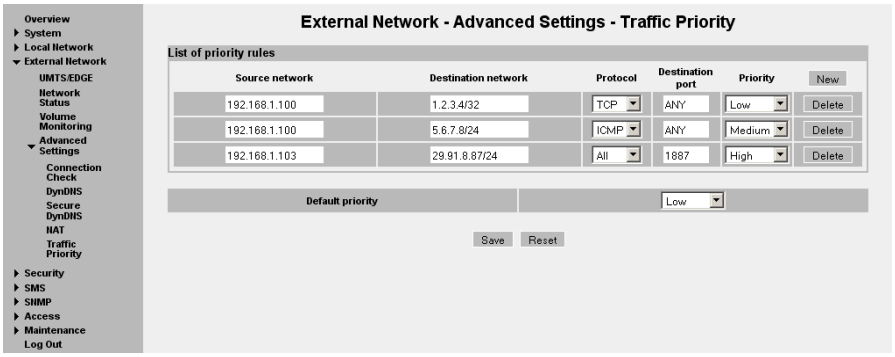
Factory setting

The factory settings for the TAINY xMOD are as follows:

Enable volume monitoring	**No (switched off)**
Maximum data volume in bytes per month	**1000000**
Send SMS when 80% of the max. data volume is reached	
Enable	**No (switched off)**
Call number	**(empty)**
Message text	**Warning:Max_Data_Volume_ reached**
Send SMS when 100% of the max. data volume is reached	
Enable	**No (switched off)**
Call number	**(empty)**
Message text	**Alert:Max_Data_Volume_ reached**

5.8 Traffic Priority

External Network > Advanced Settings > Traffic Priority



Function

This function can be used to prioritize the communication of selected data paths. If there are data in a path of high priority, they will be transmitted first. They are followed by data in paths of medium priority. Only if there are no data in path of high or medium priority, data in path of low priority are transmitted.

The data paths are defined by the IP address of the source network and the IP range of the destination network. In addition you can prioritize data of a certain type of protocol (TCP, ICMP etc.) as well as data towards a certain destination.

List of priority rules

Add an additional data path by clicking the *New* button, delete data path by clicking the *Delete* button.

Source network	Enter the source network IP address range of the data path.
Destination network	Enter the destination network IP range of the data path.
Protocol	Select the communication protocol, which shall get the level of priority.
Destination port	Enter the destination network port of the data path.
Priority	Select the priority of the data path.
Default priority	Select the priority for the default communication, for which no data path is explicitly configured.

Factory setting

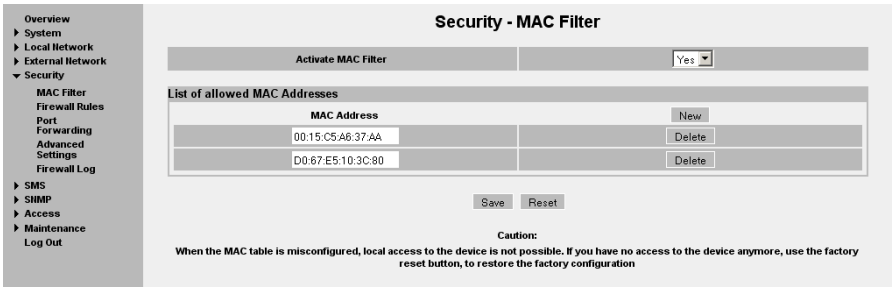
The factory settings for the TAINY xMOD are as follows:

Source network	**0.0.0.0/0**
Destination network	**0.0.0.0/0**
Protocol	**All**
Destination port	**ANY**
Priority	**Low**
Default priority	**Medium**

6 Security functions

6.1 MAC Filter

Security > MAC Filter



Function

The TAINY xMOD is equipped with a MAC filter, which allows only the communication with local applications, whose MAC addresses are registered in the TAINY xMOD.

Activate MAC Filter

Yes The MAC filter is enabled.

No The MAC filter is disabled.

List of allowed MAC Addresses

Enter the MAC address of the local applications, which may communicate with / via the TAINY xMOD.

Use *New* to add an additional MAC-Adressen and remove MAC addresses with *Delete.*

Factory setting

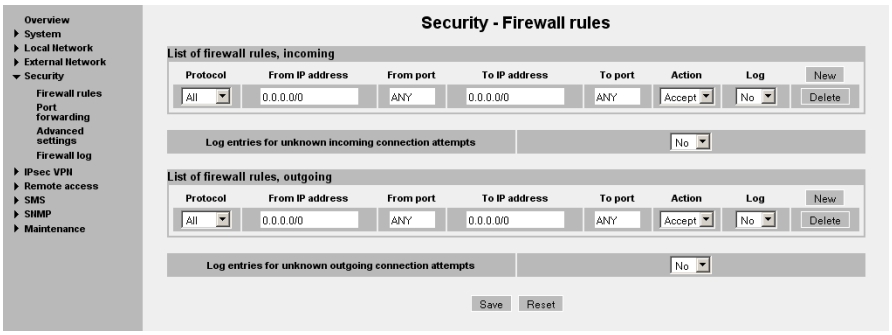
The factory settings for the TAINY xMOD are as follows:

Activate MAC Filter **No**

MAC Address **None**

6.2 Packet filter

Security > Firewall Rules



Function

The TAINY xMOD contains a stateful inspection firewall.

A stateful inspection firewall is a packet filtering method. Packet filters only let IP packets through if this has been defined previously using firewall rules. The following is defined in the firewall rules:

- which protocol (TCP, UDP, ICMP) can go through,
- the permitted source of the IP packets (From IP / From port)
- the permitted destination of the IP packets (To IP / To port)

It is likewise defined here what will be done with IP packets that are not allowed through (discard, reject).

For a simple packet filter it is always necessary to create two firewall rules for a connection:

- One rule for the query direction from the source to the destination, and
- a second rule for the query direction from the destination to the source.

It is different for a TAINY xMOD with a stateful inspection firewall. Here a firewall rule is only created for the query direction from the source to the destination. The firewall rule for the response direction from the destination to the source results from analysis of the data previously sent. The firewall rule for the responses is closed again after the responses are received or after a short time period has elapsed. Thus responses can only go through if there was a previous query. This means that the response rule cannot be used for unauthorised access. What is more, special procedures make it possible for UDP and ICMP data to also go through, even though these data were not requested before.

List of firewall rules, incoming

The Firewall Rules (incoming) are used to define how to handle IP packets that are received from external networks (e.g. the Internet) via UMTS/GPRS. The source is the sender of this IP packet. The destination is the local applications on the TAINY xMOD.

In the factory setting, no incoming firewall rule is set initially, i.e. no IP packets can go through.

New Adds an additional firewall rule that you can then fill out.

Delete Removes firewall rules that have been created.

Protocol Select the protocol for which this rule will be valid. The following selections are available: *TCP, UDP* and *ICMP*. If you select *All*, the rule is valid for all three protocols.

Note

If you select *All* or *ICMP* for protocol, a port assignment is not effective.

From IP address Enter the IP address of the external remote station that is allowed to send IP packets to the local network. Do this by specifying the IP address or an IP range for the remote station. ***0.0.0.0/0*** means all addresses.

To specify a range, use the CIDR notation - see Chapter 16.

From port Enter the port (e.g. 80) or a port range (e.g. 8080:9090) from which the external remote station is allowed to send IP packets.

(is only evaluated for the protocols TCP and UDP)

To IP address Enter the IP address in the local network to which IP packets may be sent. Do this by specifying the IP address or an IP range of the application in the local network. ***0.0.0.0/0*** means all addresses.

To specify a range, use the CIDR notation - see Chapter 16.

To port Enter the port (e.g. 80) or a port range (e.g. 8080:9090) to which the external remote station is allowed to send IP packets.

Action Select how incoming IP packets are to be handled:

Accept – The data packets can go through,

Reject – The data packets are rejected, and the sender receives a corresponding message.

Drop – The data packets are discarded without any feedback to the sender.

List of firewall rules, outgoing

The Firewall Rules (outgoing) are used to define how to handle IP packets that are received from the local network. The source is an application in the local network. The destination is an external remote station, e.g. on the Internet or in a private network.

In the factory setting, no outgoing firewall rule is set initially, i.e. no IP packets can go through.

New Adds an additional firewall rule that you can then fill out.

Protocol Select the protocol for which this rule will be valid. The following selections are available: *TCP, UDP* and *ICMP*. If you select *All*, the rule is valid for all three protocols.

From IP address Enter the IP address of the local application that is allowed to send IP packets to the external network. Do this by specifying the IP address or an IP range for the local application. ***0.0.0.0/0*** means all addresses.

To specify a range, use the CIDR notation - see Chapter 16.

From port Enter the port from which the local network is allowed to send IP packets. Do this by specifying the port number.

(is only evaluated for the protocols TCP and UDP)

To IP address Enter the IP address in the external network to which IP packets may be sent. Do this by specifying the IP address or an IP range of the application in the network. ***0.0.0.0/0*** means all addresses.

To specify a range, use the CIDR notation - see Chapter 16.

To port Enter the port to which the external local application is allowed to send IP packets. Do this by specifying the port number.

(is only evaluated for the protocols TCP and UDP)

Action Select how outgoing IP packets are to be handled:

Accept – The data packets can go through,

Reject – The data packets are rejected, and the sender receives a corresponding message.

Drop – The data packets are discarded without any feedback to the sender.

List of firewall rules, incoming/outgoing

Log For each individual firewall rule you can define whether the event should be

- logged when the rule takes effect - set *Log* to *Yes*
- or not - set *Log* to *No* (factory setting)

The log is kept in the firewall log, see Chapter 6.5.

Log entries for unknown incoming/ outgoing connection attempts

This logs all connection attempts that are not covered by the defined rules. This function can be enabled or disabled separately for incoming and outgoing connection attempts.

Factory setting

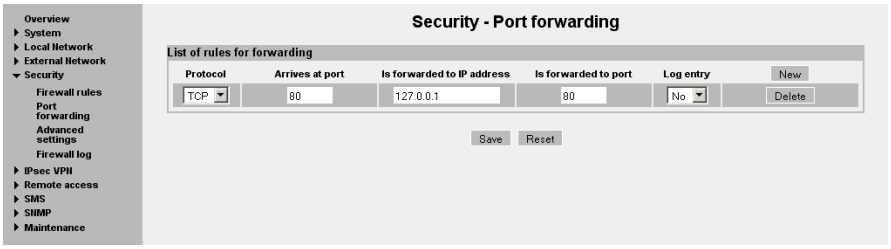
The factory settings for the TAINY xMOD are as follows:

Incoming firewall	List of firewall rules, incoming	**- (Everything blocked)**
	Protocol	**All**

	From IP address	**0.0.0.0/0**
	From port	**ANY**
	To IP address	**0.0.0.0/0**
	To port	**ANY**
	Action	**Accept**
	Log	**No (switched off)**
	Log entries for unknown incoming connection attempts	**No (switched off)**
Outgoing firewall	List of firewall rules, outgoing	**- (Everything blocked)**
	Protocol	**All**
	From IP address	**0.0.0.0/0**
	From port	**ANY**
	To IP address	**0.0.0.0/0**
	To port	**ANY**
	Action	**Accept**
	Log	**No (switched off)**
	Log entries for unknown outgoing connection attempts	**No (switched off)**

6.3 Port forwarding

Security > Port Forwarding



Function

If a rule has been created for port forwarding, then data packets received at a defined IP port of the TAINY xMOD from the external network will be forwarded. The incoming data packets are then forwarded to a specified IP address and port number in the local network. The port forwarding can be configured for TCP or UDP.

In port forwarding the following occurs: The header of incoming data packets from the external network that are addressed to the external IP address of the TAINY xMOD and to a specific port are adapted so that they are forwarded to the internal network to a specific computer and to a specific port of that computer.
This means that the IP address and port number in the header of incoming data packets are modified.

This process is also called Destination NAT or Port Forwarding.

Note

In order for incoming data packets to be forwarded to the defined IP address in the local network, a corresponding incoming firewall rule must be set up for this IP address in the packet filter. See Chapter 6.1.

New Adds a new rule for forwarding that you can then fill out.

Delete Removes rules for forwarding that have been created.

Protocol	Specify here the protocol (TCP or UDP) to which the rule should refer.
Arrives at port	Specify here the port number (e.g. 80) at which the data packets which are to be forwarded arrive from the external network.
Is forwarded to IP address	Specify here the IP address in the local network to which the incoming data packets should be forwarded.
Is forwarded to port	Specify here the port number (e.g. 80) for the IP address in the local network to which the incoming data packets should be forwarded.
Log entry	For each port forwarding rule you can define whether the event should be - logged when the rule takes effect - set *Log entry* to *Yes* - or not - set *Log entry* to *No* (factory setting) The log is kept in the firewall log, see Chapter 6.5.

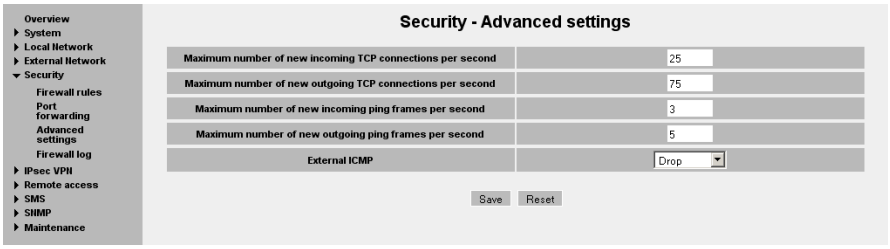
Factory setting

The factory settings for the TAINY xMOD are as follows:

List of rules for forwarding	**-**
Protocol	**TCP**
Arrives at port	**80**
Is forwarded to IP address	**127.0.0.1**
Is forwarded to port	**80**
Log entry	**No (switched off)**

6.4 Advanced security functions

Security > Advanced Settings



Function

The advanced security functions serve to protect the TAINY xMOD and the local applications against attacks. For protective purposes it is assumed that only a certain number of connections or received ping packets are permissible and desirable in normal operation, and that a sudden burst represents an attack.

Maximum number …

The entries

Maximum number of new incoming TCP connections per second

Maximum number of new outgoing TCP connections per second

Maximum number of new incoming ping frames per second

Maximum number of new outgoing ping frames per second

External ICMP

set the upper limits. The settings (see illustration) have been selected so that they will in practice never be reached in normal use. In the event of an attack, however, they can be reached very easily, which means that the limitations constitute additional protection. If your operating environment contains special requirements, then you can change the values accordingly.

External ICMP

You can use this option to affect the response when ICMP packets are received that are sent from the external network in the direction of the TAINY xMOD. You have the following options:

Drop: All ICMP packets to the TAINY xMOD are discarded.

Allow ping: Only ping packets (ICMP type 8) to the TAINY xMOD are accepted.

Accept: All types of ICMP packets to the TAINY xMOD are accepted.

Factory setting

The factory settings for the TAINY xMOD are as follows:

Maximum number of new incoming TCP connections per second	**25**
Maximum number of new outgoing TCP connections per second	**75**
Maximum number of new incoming ping frames per second	**3**
Maximum number of new outgoing ping frames per second	**5**
External ICMP	**Drop**

6.5 Firewall log

Security > Firewall Log

Function

The application of individual firewall rules is recorded in the firewall log. To do this, the LOG function must be activated for the various firewall functions.

Caution

The firewall log is lost in the event of a reboot.

7 IPsec-VPN connections

ONLY TAINY xMOD-V3

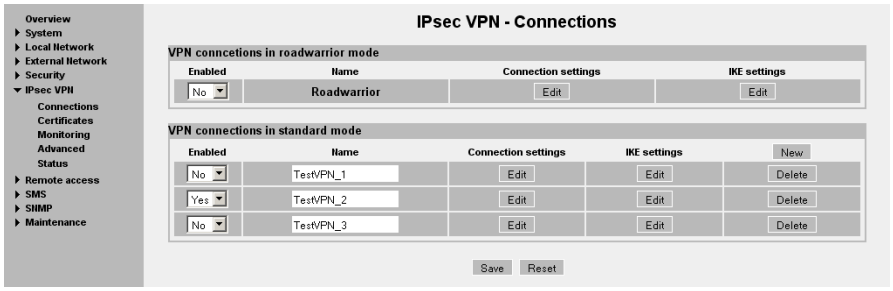
Note regarding the scope of function

The menu item IPsec-VPN is only present with TAINY xMOD-V3 devices. Only the TAINY xMOD-V3 support IPsec-VPN connections.

7.1 Introduction

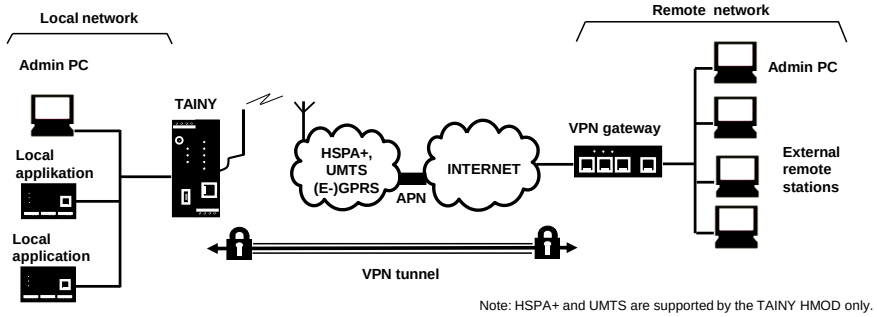
IPsec VPN > Connections

ONLY TAINY xMOD-V3



Function

The TAINY xMOD-V3 can connect the local network to a friendly remote network via a VPN tunnel. The IP data packets that are exchanged between the two networks are encrypted, and are protected against unauthorised tampering by the VPN tunnel. This means that even unprotected public networks like the Internet can be used to transfer data without endangering the confidentiality or integrity of the data.



Note: HSPA+ and UMTS are supported by the TAINY HMOD only.

For the TAINY xMOD-V3 to establish a VPN tunnel, the remote network must have a VPN gateway as the remote station for the TAINY xMOD-V3

For the VPN tunnel, the TAINY xMOD-V3 uses the IPsec method in tunnel mode. In this method the IP data packets to be transmitted are completely encrypted and provided with a new header before they are sent to the remote station's VPN gateway. There the data packets are received, decrypted, and used to reconstruct the original data packets. These are then forwarded to their destination in the remote network.

Differences between two VPN connection modes:

- In VPN Roadwarrior Mode the TAINY xMOD-V3 VPN can accept connections from remote stations with an unknown address. These can be, for example, remote stations in mobile use that obtain their IP address dynamically. The TAINY xMOD-V3 must have a permanent IP address or must be accessible via a DynDNS service (see 5.3 and 5.4.)
  The VPN connection must be established by the remote station. Only one VPN connection is possible in Roadwarrior Mode. VPN connections in Standard Mode can be used at the same time.
- In VPN Standard Mode the address (IP address or host name) of the remote station's VPN gateway must be known for the VPN connection to be established. The VPN connection can be established either by the TAINY xMOD-V3 or by the remote station's VPN gateway as desired.

Establishment of the VPN connection is subdivided into two phases: First in Phase 1 (ISAKMP = Internet Security Association and Key Management Protocol) the Security Association (SA) for the key exchange between the TAINY xMOD-V3 and the VPN gateway of the remote station is established.

After that in Phase 2 (IPsec = Internet Protocol Security) the Security Association (SA) for the actual IPsec connection between the TAINY xMOD-V3 and the remote station's VPN gateway is established.

Requirements for the remote network's VPN gateway

In order to successfully establish an IPsec connection, the VPN remote station must support IPsec with the following configuration:

- Authentication via X.509 certificates, CA certificates or pre shared key (PSK)
- ESP
- Diffie-Hellman group 1, 2 or 5
- 3DES or AES encryption
- MD5 or SHA-1 hash algorithms
- Tunnel Mode
- Quick Mode
- Main Mode
- SA Lifetime (1 second to 24 hours)

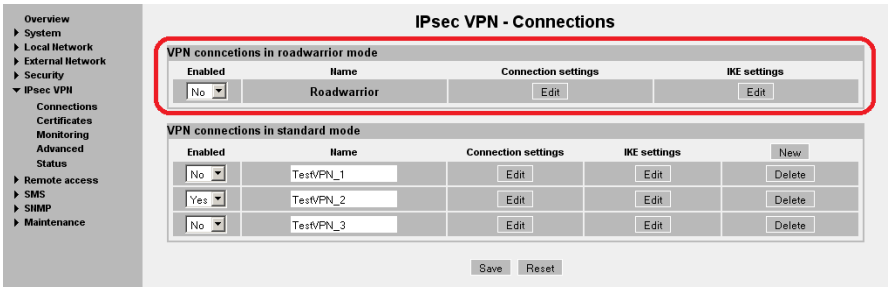
If the remote station is a computer running under Windows 2000, then the Microsoft Windows 2000 High Encryption Pack or at least Service Pack 2 must also be installed.

If the remote station is on the other side of a NAT router, then the remote station must support NAT-T. Or else the NAT router must know the IPsec protocol (IPsec/VPN passthrough).

7.2 IPsec VPN roadwarrior mode

IPsec VPN > Connections

ONLY TAINY xMOD-V3

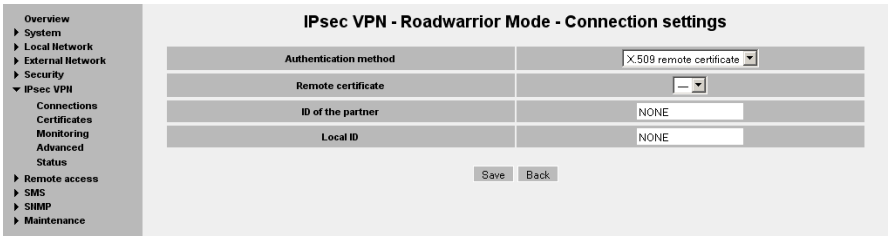


Function

The Roadwarrior Mode makes it possible for the TAINY xMOD-V3 to accept a VPN connection initiated by a remote station with an unknown IP address. The remote station must authenticate itself properly; in this VPN connection there is no identification of the remote station based on the IP address or the host name of the remote station.

Roadwarrior mode

Edit Connection settings



Function

Set the TAINY xMOD-V3 up in accordance with what has been agreed with the system administrator of the remote station.

Authentication method

Select the authentication method in accordance with what you have agreed with the system administrator of the remote station.

The TAINY xMOD-V3 supports three methods:

- X.509 remote certificate
- CA certificate
- Pre shared key

X.509 certificate, CA certificate

In the authentication methods X.509 certificate and CA certificate, the keys used for authentication have first been signed by a Certification Authority (CA). This method is considered especially secure. A CA can be a service provider, but also, for example, the system administrator for your project, provided that he has the necessary software tools. The CA creates a certificate file (PKCS12) with the file extension *p12 for each of the two remote stations. This certificate file contains the public and private keys for the own station, the signed certificate from the CA, and the public key of the CA. For the authentication method X.509 there is additionally a key file (*.pem or *.crt) for each of the two remote stations with the public key of the own station.

X.509 certificate

The public keys (files with extension *.pem or *.crt) are exchanged between the TAINY xMOD-V3 and the remote station's VPN gateway takes place manually,

for example on a CD-ROM or via e-mail. To load the certificate, proceed as described in Chapter 7.4.

CA certificate — The public keys are exchanged between the TAINY xMOD-V3 and the remote station's VPN gateway via the data connection when the VPN connection is established. Manual exchange of the key files is not necessary.

Pre shared key (PSK)

This method is primarily supported by older IPsec implementations. Here authentication is performed with a character string agreed on beforehand. In order to obtain high security, the character string should consist of about randomly-selected 30 lower-case and upper-case letters and numerals.

The following characters are permitted:

! $ % & ' ( ) * + , . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ ` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } #

Entered characters cannot be read.

Remote certificate — If you have selected *X.509 remote certificate* as the authentication method, then a list of the remote certificates that you have already loaded into the TAINY xMOD-V3 is displayed here. Select the certificate for the VPN connection.

ID of the partner

Local ID — The *Local ID* and the *ID of the partner* are used by IPsec to identify the remote stations uniquely when establishing the VPN connection. The own *Local ID* constitutes the *ID of the partner* of the remote station and vice versa.

For authentication with X.509 certificate or CA certificate:

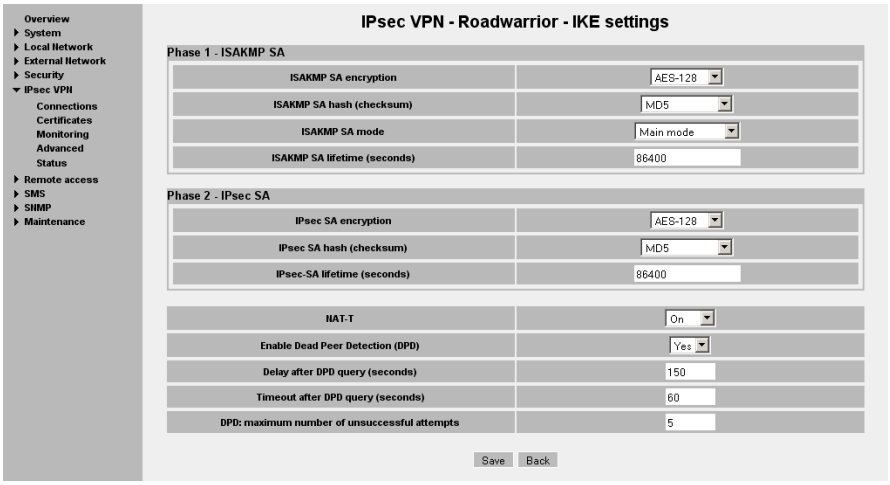
- If you keep the factory setting *NONE*, then the Distinguished Names from the own certificate and from the certificate communicated by the remote station are automatically used as the *Local ID* and *ID of the partner*.
- If you manually change the entry for the *Local ID* or the *ID of the partner*, then the corresponding entries must be adapted at the remote station. The manual entry for *Local ID* or *ID of the partner* must be made in the ASN.1 format, e.g. "C=XY/O=XY Org/CN=xy.org.org"

For authentication with pre shared key (PSK):

- In Roadwarrior Mode the *ID of the partner* must be entered manually. The *ID of the partner* must have the format of a host name (e.g. RemoteStation.de) or the format of an e-mail address (remote@station.de), and must be the same as the *Local ID* of the remote station.
  The *Local ID* can be left on *NONE*. In this case the IP address is used as the local IP address. If you enter a *Local ID*, then it must have the format of a host name (e.g. RemoteStation.de) or the format of an e-mail address (remote@station.de), and must be the same as the *ID of the partner* of the remote station.
-

Roadwarrior mode

Edit IKE



Function

Here you can define the properties of the VPN connection according to your requirements and what you have agreed with the system administrator of the remote station.

ISAKMP SA encryption

IPsec SA encryption

Agree with the administrator of the remote station which encryption method will be used for the ISAKMP SA and the IPsec-SA. The TAINY xMOD-V3 supports the following methods:

- 3DES-168
- AES-128
- AES-192
- AES-256

AES-128 is the most frequently used method, and is therefore set as the default.

The method can be defined differently for ISAKMP SA and IPsec-SA.

Note:
The more bits in the encryption algorithm - indicated by the appended number - the more secure it is. The method AES-256 is therefore considered the most secure. However, the longer the key, the more time the encryption process takes and the more computing power is required.

ISAKMP SA hash

IPsec SA hash

Agree with the administrator of the remote station which method will be used for computing checksums/hashes during the ISAKMP phase and the IPsec phase. The following selections are available:

- MD5 or SHA-1 (automatic detection)
- MD5
- SHA-1

The method can be defined differently for ISAKMP SA and IPsec-SA.

ISAKMP SA mode

Agree with the administrator of the remote station which method will be used for negotiating the ISAKMP-SA. The following selections are available:

- Main mode

- Aggressive mode

Note:

If the authentication method Pre shared key is used, *Aggressive mode* must be set in Roadwarrior mode.

ISAKMP SA lifetime

IPsec SA lifetime

The keys for an IPsec connection are renewed at certain intervals in order to increase the effort required to attack an IPsec connection.

Specify the lifetime (in seconds) of the keys agreed on for the ISAKMP SA and IPsec SA.

The lifetime can be defined differently for ISAKMP SA and IPsec SA.

NAT-T

There may be a NAT router between the TAINY xMOD-V3 and the VPN gateway of the remote network. Not all NAT routers allow IPsec data packets to go through. It may therefore be necessary to encapsulate the IPsec data packets in UDP packets so that they can go through the NAT router.

On: If the TAINY xMOD-V3 detects a NAT router that does not let the IPsec data packets through, then UDP encapsulation is started automatically.

Force: During negotiation of the connection parameters for the VPN connection, encapsulated transmission of the data packets during the connection is insisted upon.

Off: The NAT-T function is switched off

Enable dead peer detection

If the remote station supports the dead peer detection (DPD) protocol, then the partner in question can detect whether the IPsec connection is still valid or not, meaning that it may have to be re-established. Without DPD, depending on the configuration it may be necessary to wait until the SA lifetime elapses or the connection has to be re-initiated manually. To check whether the IPsec connection is still valid, the dead peer detection sends DPD requests to the remote station itself. If there is no answer, then after the permitted number of failed attempts the IPsec connection is considered to be interrupted.

Warning

Sending the DPD requests and using NAT-T increases the amount of data sent and received over the mobile data service connection (HSPA+, UMTS, EGPRS and GPRS). Depending on the selected settings, the additional data traffic can amount to 5 Mbyte per month or more. This can lead to additional costs.

Yes Dead peer detection is switched on. Independently of the transmission of user data, the TAINY xMOD-V3 detects if the connection is lost, in which case it waits for the connection to be re-established by the remote stations.

No Dead peer detection is switched off

Delay after DPD query (seconds)

Time period in seconds after which DPD requests will be sent. These requests test whether the remote station is still available.

Timeout after DPD query (seconds)

Duration of time in seconds after which a DPD query shall be considered unsuccessful, if no response to the DPD query is received. If a DPD query is unsuccessful, this is also the interval for the delay before the subsequent query is sent, until the connection is ultimately declared as disconnected or the TAINY xMOD receives a DPD response again.

DPD: maximum number of unsuccess-

Number of failed attempts permitted before the IPsec connection is considered to be interrupted.

ful attempts

Factory setting

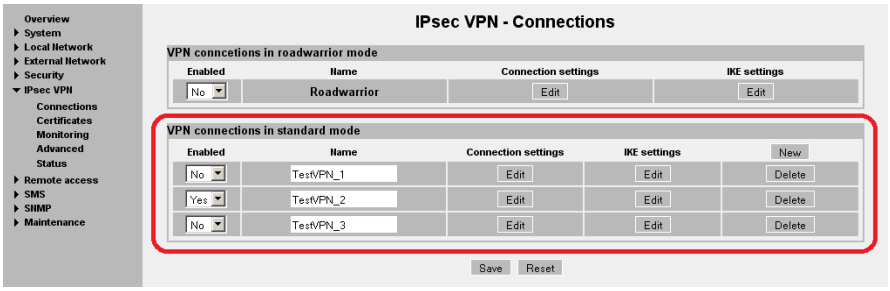
The factory settings for the TAINY xMOD-V3 are as follows:

Name	**Roadwarrior**
Enabled	**No (switched off)**
Authentication method	**CA certificate**
ID of the partner	**NONE**
Local ID	**NONE**
Remote certificate	**-**
Pre shared key	**NONE**
ISAKMP SA encryption	**AES-128**
ISAKMP SA hash (checksum)	**MD5**
ISAKMP SA mode	**Main mode**
ISAKMP SA lifetime (seconds)	**86400**
IPsec SA encryption	**AES-128**
IPsec SA hash (checksum)	**MD5**
IPsec SA lifetime (seconds)	**86400**
NAT-T	**On**
Enable Dead Peer Detection	**Yes**
Delay after DPD query (seconds)	**150**
Timeout after DPD query (seconds)	**60**
DPD: maximum number of unsuccessful attempts	**5**

7.3 IPsec VPN Standard mode

IPsec VPN > Connections

ONLY TAINY xMOD-V3

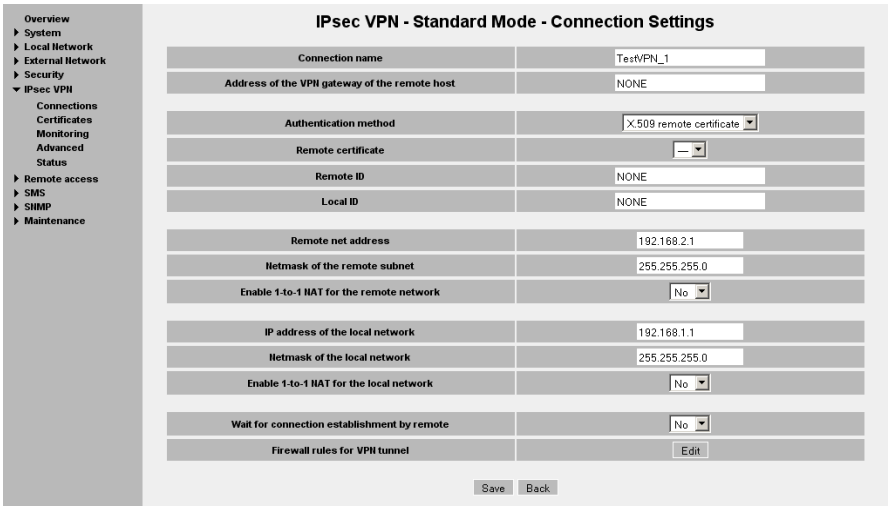


Function

The VPN connections already created are shown. You can enable (Enabled = *Yes*) or disable (Enabled = *No*) each individual connection. You can use *New* to add additional VPN connections, *Edit Settings* and *IKE Settings* to set them up, and *Delete* to remove a connection.

VPN Standard mode

Edit Connection settings

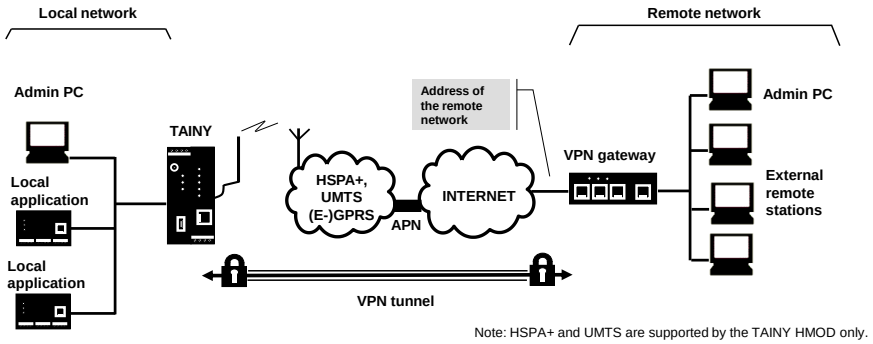


Connection Name

Give the new connection a connection name here.

Address of the VPN gateway of the remote host

Specify the address of the remote station here, either as a host name (e.g. myaddress.com) or as an IP address.



Note: HSPA+ and UMTS are supported by the TAINY HMOD only.

Authentication method

Select the authentication method in accordance with what you have agreed with the system administrator of the remote station.

The TAINY xMOD-V3 supports three methods:

- X.509 remote certificate
- CA certificate
- Pre shared key

X.509 remote certificate, CA certificate

In the authentication methods X.509 certificate and CA certificate, the keys used for authentication have first been signed by a Certification Authority (CA). This method is considered especially secure. A CA can be a service provider, but also, for example, the system administrator for your project, provided that he has the necessary software tools. The CA creates a certificate file (PKCS12) with the file extension *p12 for each of the two remote stations. This certificate file contains the public and private keys for the own station, the signed certificate from the CA, and the public key of the CA. For the authentication method X.509 there is additionally a key file (*.pem or *.crt) for each of the two remote stations with the public key of the own station.

X.509 remote certificate	The public keys (files with extension *.pem or *.crt) are exchanged between the TAINY xMOD-V3 and the remote station's VPN gateway takes place manually, for example on a CD-ROM or via e-mail. To load the certificate, proceed as described in Chapter 7.4.
CA certificate	The public keys are exchanged between the TAINY xMOD-V3 and the remote station's VPN gateway via the data connection when the VPN connection is established. Manual exchange of the key files is not necessary.

Pre shared key (PSK)

This method is primarily supported by older IPsec implementations. Here authentication is performed with a character string agreed on beforehand. In order to obtain high security, the character string should consist of about randomly-selected 30 lower-case and upper-case letters and numerals.

The following characters are permitted:

! $ % & ' ( ) * + , . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ ` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } #

The entry is concealed.

Remote certificate

If you have selected *X.509 remote certificate* as the authentication method, then a list of the remote certificates that you have already loaded into the TAINY xMOD-V3 is displayed here. Select the certificate for the VPN connection.

Remote ID

Local ID

The *Local ID* and the *Remote ID* are used by IPsec to identify the remote stations uniquely when establishing the VPN connection.

For authentication with X.509 certificate or CA certificate:

- If you keep the factory setting *NONE*, then the Distinguished Names from the own certificate and from the certificate communicated by the remote station are automatically applied and used as the *Local ID* and *Remote ID*.
- If you manually change the entry for the *Local ID* or the *Remote ID*, then the corresponding entries must be adapted at the remote station. The own *Local ID* must be the same as the *Remote ID* of the remote station and vice versa. The entries for *Local IDs* or *Remote IDs* must be made in the ASN.1 format, e.g. "C=XY/O=XY Org/CN=xy.org.org"

For authentication with pre shared key (PSK):

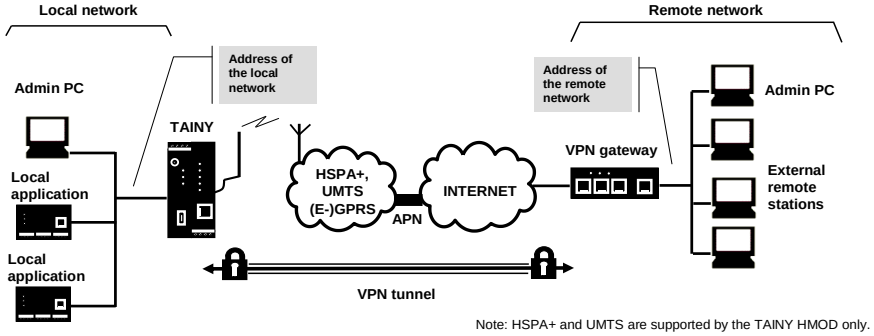
- If you keep the factory setting *NONE*, then the own IP address is automatically used as the *Local ID*, and the IP address of the remote station is used as the *Remote ID*:
- If you manually change the entry for the *Local ID* or for the *Remote ID*, then the entries must have the format of a host name (e.g. RemoteStation.de) or the format of an e-mail address (remote@station.de). The own *Local ID* must be the same as the *Remote ID* of the remote station and vice versa.

Note:

If with pre shared key (PSK) the IP address is not used as the *Remote ID*, then the *Aggressive Mode* has to be set as the ISAKMP SA mode.

Remote net address

Here enter the IP address (e.g. 123.123.123.123) of the remote network. The remote network can also be only a single computer.



Note: HSPA+ and UMTS are supported by the TAINY HMOD only.

Netmask of the remote subnet

Here enter the subnet mask (e.g. 255.255.255.0) of the remote network. The remote network can also be only a single computer.

Enable 1-to-1 NAT for the remote network

The TAINY xMOD-V3 has a 1-to-1 NAT function for the remote network.

In TAINY xMOD-V3, the address range of the remote network on the VPN connection is defined by the

- IP address of the remote network (*Remote net address*) and the
- *Netmask of the remote subnet*

If 1-to-1 NAT is switched off, local applications must use this address range for the addressing of remote locations in the remote network.

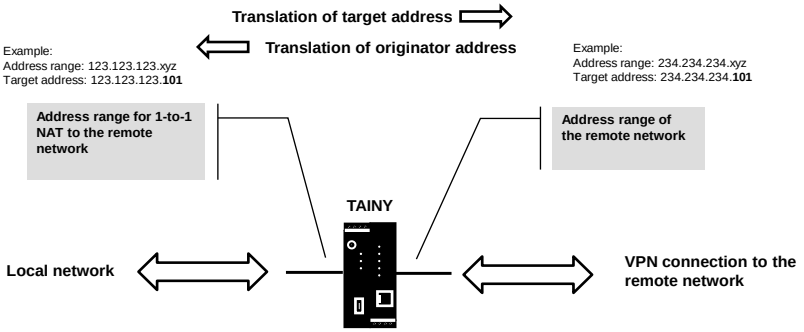
A locally used address range through which the local applications can

address the remote locations in the remote network can be defined when 1-to-1 NAT is activated.

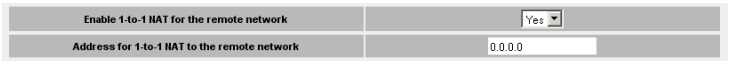
The 1-to-1 NAT function in TAINY xMOD-V3 then maps the locally defined address range of the remote network on the address range of the remote network on the VPN connection.

The locally used address range of the remote network is defined by the

- *Address for 1-to-1 NAT to the remote network* and the
- *Netmask of the remote subnet*



Yes The TAINY xMOD-V3 uses 1-to-1 NAT for the remote network.



Enter the locally used target address as the address for 1-to-1 NAT for the remote network.

No The TAINY xMOD-V3 does not use 1-to-1 NAT for the remote network.

IP address of the local network

Here enter the IP address (e.g. 123.123.123.123) of the local network. The local network can also be only a single computer.

Netmask of the local network

Here enter the subnet mask (e.g. 255.255.255.0) of the local network. The local network can also be only a single computer.

Enable 1-to-1 NAT for the local network

In TAINY xMOD-V3, the address range of the local network on the VPN connection is defined by the

- *IP address of the local network* and the
- *Netmask of the local network*

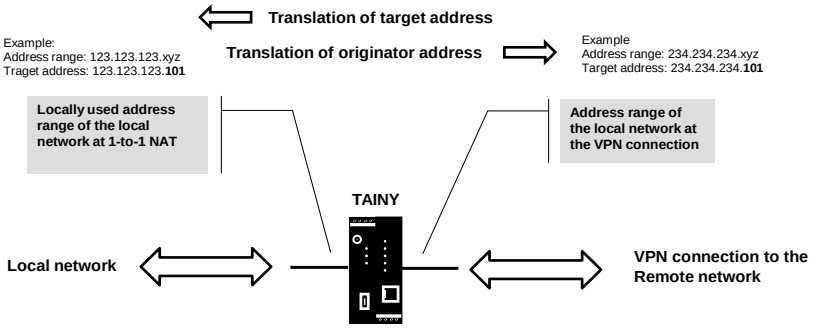
If 1-to-1 NAT is disabled, the addresses of local application must be within this address range, that they can be addressed via the VPN connection by the remote stations within the remote network.

If 1-to-1 NAT is activated, a locally used address range for the local network can be defined, which may differ from the address range used at the VPN connection.

The 1-to-1 NAT function of the TAINY xMOD-V3 maps the local address range of the local network into the address range of the VPN connection.

The locally used address range of the local network is defined by the

- *Address for 1-to-1-NAT in the local network* and the
- *Netmask of the local network*



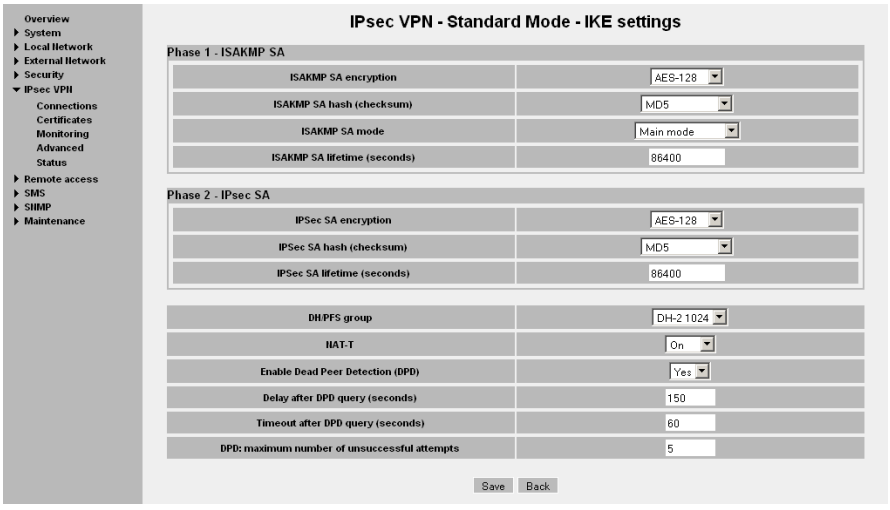
	Yes	The TAINY xMOD-V3 uses 1-to-1-NAT to the local network.

Enter as the *Address for 1-to-1-NAT in the local network* the locally used target address.

	No	The TAINY xMOD-V3 does not use 1-to-1-NAT to the local network.
Wait for connection establishment by remote	*Yes*	The TAINY xMOD-V3 waits for the VPN gateway of the remote network to initiate establishment of the VPN connection.
	No	The TAINY xMOD-V3 initiates establishment of the connection.
Firewall rules for VPN tunnel	See Chapter 7.5.	

VPN Standard mode

Edit IKE



Function	Here you can define the properties of the VPN connection according to your requirements and what you have agreed with the system administrator of the remote station.
ISAKMP SA encryption	Agree with the administrator of the remote station which encryption method will be used for the ISAKMP SA and the IPsec SA. The TAINY xMOD-V3 supports the following methods:

IPsec SA encryption

- 3DES-168
- AES-128
- AES-192
- AES-256

AES-128 is the most frequently used method, and is therefore set as the default.

The method can be defined differently for ISAKMP SA and IPsec-SA.

Note
The more bits in the encryption algorithm - indicated by the appended number - the more secure it is. The method AES-256 is therefore considered the most secure. However, the longer the key, the more time the encryption process takes and the more computing power is required.

ISAKMP SA hash

IPsec SA hash

Agree with the administrator of the remote station which method will be used for computing checksums/hashes during the ISAKMP phase and the IPsec phase. The following selections are available:

- MD5 or SHA-1 (automatic detection)
- MD5
- SHA-1

The method can be defined differently for ISAKMP SA and IPsec-SA.

ISAKMP SA mode

Agree with the administrator of the remote station which method will be used for negotiating the ISAKMP SA. The following selections are available:

- Main mode
- Aggressive mode

ISAKMP SA lifetime

IPsec SA lifetime

The keys for an IPsec connection are renewed at certain intervals in order to increase the effort required to attack an IPsec connection.

Specify the lifetime (in seconds) of the keys agreed on for the ISAKMP SA and IPsec-SA.

The lifetime can be defined differently for ISAKMP SA and IPsec-SA.

DH/PFS group

Agree with the administrator of the remote station the DH group for the key exchange.

NAT-T

There may be a NAT router between the TAINY xMOD-V3 and the VPN gateway of the remote network. Not all NAT routers allow IPsec data packets to go through. It may therefore be necessary to encapsulate the IPsec data packets in UDP packets so that they can go through the NAT router.

On:	If the TAINY xMOD-V3 detects a NAT router that does not let the IPsec data packets through, then UDP encapsulation is started automatically.
Force:	During negotiation of the connection parameters for the VPN connection, encapsulated transmission of the data packets during the connection is insisted upon.
Off:	The NAT-T function is switched off

Enable Dead Peer Detection (DPD)

If the remote station supports the dead peer detection (DPD) protocol, then the partner in question can detect whether the IPsec connection is still valid or not, meaning that it may have to be re-established. Without DPD, depending on the configuration it may be necessary to wait until the SA lifetime elapses or the connection has to be re-initiated manually. To check whether the IPsec connection is still valid, the dead peer detection sends DPD requests to the remote station itself. If there is no answer, then after the permitted number of failed attempts the IPsec connection is considered to be interrupted.

Warning

Sending the DPD requests and using NAT-T increases the amount of data sent and received over the mobile data service connection (HSPA+, UMTS, EGPRS and GPRS). Depending on the selected settings, the additional data traffic can amount to 5 Mbyte per month or more. This can lead to additional costs.

Yes	Dead peer detection is switched on. Attempts are made to re-establish the IPsec connection if it has been declared dead, independently of the transmission of user data.
No	Dead peer detection is switched off

Delay after DPD query (seconds)

Time period in seconds after which DPD requests will be sent. These requests test whether the remote station is still available.

Timeout after DPD query (seconds)

Duration of time in seconds after which a DPD query shall be considered unsuccessful, if no response to the DPD query is received. If a DPD query is unsuccessful, this is also the interval for the delay before the subsequent query is sent, until the connection is ultimately declared as disconnected or the TAINY xMOD receives a DPD response again.

DPD: maximum number of unsuccessful attempts

Number of failed attempts permitted before the IPsec connection is considered to be interrupted.

Factory setting

The factory settings used by the TAINY xMOD-V3 for a newly created connection are as follows:

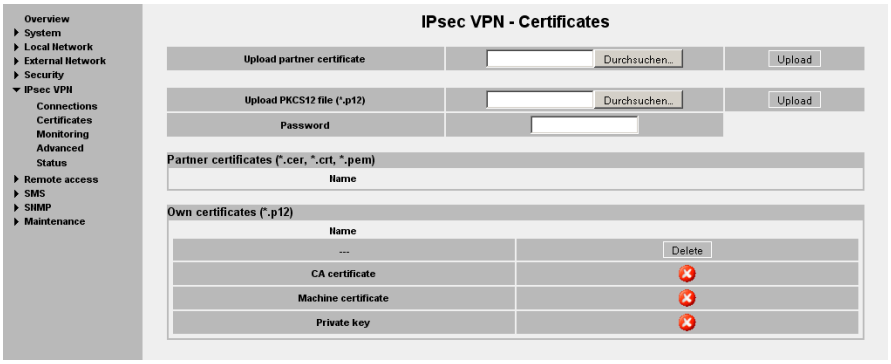
Enabled	**No (switched off)**
Name / Connection name	**NewConnection**
Address of the VPN gateway of the remote host	**NONE**
Authentication method	**CA certificate**
Remote certificate	**-**
Pre shared key	**NONE**
Remote ID	**NONE**
Local ID	**NONE**
Remote net address	**192.168.2.1**
Netmask of the remote subnet	**255.255.255.0**
Enable 1-to-1 NAT for the remote network	**No**
Address for 1-to-1 NAT to the remote network	**0.0.0.0**
IP address of the local network	**192.168.1.1**

Netmask of the local network	**255.255.255.0**
Enable 1-to-1 NAT for the local network	**No**
Address for 1-to-1 NAT in the local network	**0.0.0.0**
Wait for connection establishment by remote	**No**
ISAKMP SA encryption	**AES-128**
ISAKMP SA hash (checksum)	**MD5**
ISAKMP SA mode	**Main mode**
ISAKMP SA lifetime (seconds)	**86400**
IPsec SA encryption	**AES-128**
IPsec SA hash (checksum)	**MD5**
IPsec SA lifetime (seconds)	**86400**
DH/PFS group	**DH-2 1024**
NAT-T	**On**
Enable Dead Peer Detection (DPD)	**Yes**
Delay after DPD query (seconds)	**150**
Timeout after DPD query (seconds)	**60**
DPD: maximum number of unsuccessful attempts	**5**

7.4 Loading VPN certificates

IPsec VPN > Certificates

ONLY TAINY xMOD-V3



Function	Loading and administering certificates and keys.
Upload partner certificate	Here load key files (*.pem, *.crt) with remote certificates and public key from remote stations into the TAINY xMOD-V3. To do this, the files must be saved on the Admin PC. A remote partner certificate is only required for the authentication method with X.509 certificate.
Upload PKCS12 file (*.p12)	Here load the certificate file (PKCS12 file) with the file extension .p12 into the TAINY xMOD-V3. To do this, the certificate file must be saved on the Admin PC.

Caution

If there is already a certificate file in the device, then it must be deleted before loading a new file.

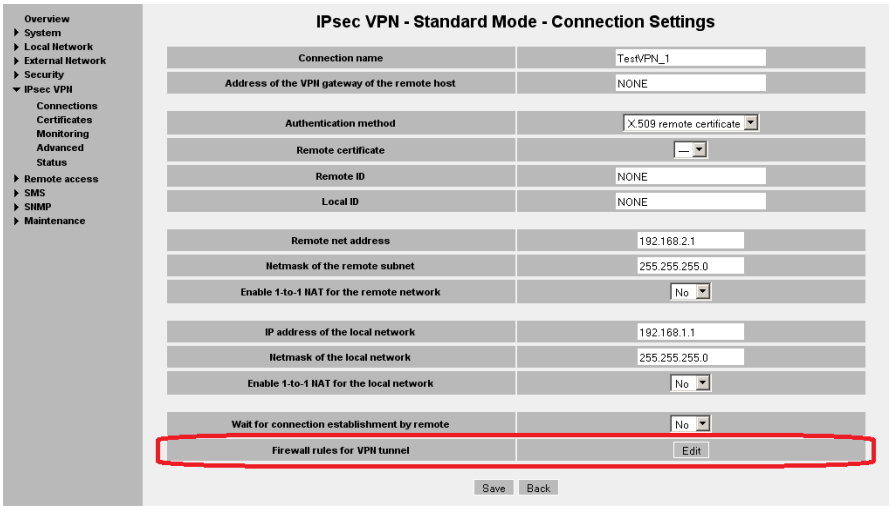
Password	The certificate file (PKCS12 file) is password-protected. Here enter the password that you received with the certificate file.
Partner certificates (*.cer, *.crt, *.pem)	A list with all of the loaded remote certificates is shown here. You can use *Delete* to remove a remote certificate that is no longer needed.
Own certificates (*.p12)	The name and status of the loaded certificate file (PKCS12 file) is shown here. The corresponding component of the certificate file is present The corresponding component is missing or the wrong password was entered.

7.5 Firewall rules for VPN tunnel

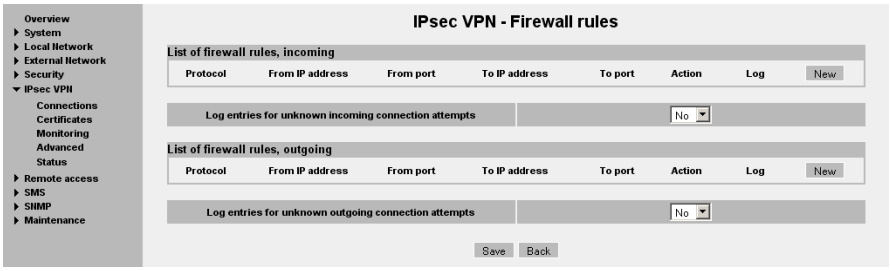
Firewall rules for VPN tunnel

The user interface for setting up the firewall rules for VPN tunnels can be found under IPsec VPN > Connections:

ONLY TAINY xMOD-V3



IPsec VPN – Edit Firewall rules



Function

The IPsec VPN connection is viewed as fundamentally secure. Thus data traffic over this connection is not limited by default. It is possible, however, to create firewall rules for the VPN connection

To set up firewall rules for the VPN connection, proceed in the same way as for setting up the packet filter function of the general firewall (see Chapter 6.1). However, the rules defined here apply only to the specific VPN connection.

Factory setting

The factory settings used by the TAINY xMOD-V3 for a newly created connection are as follows:

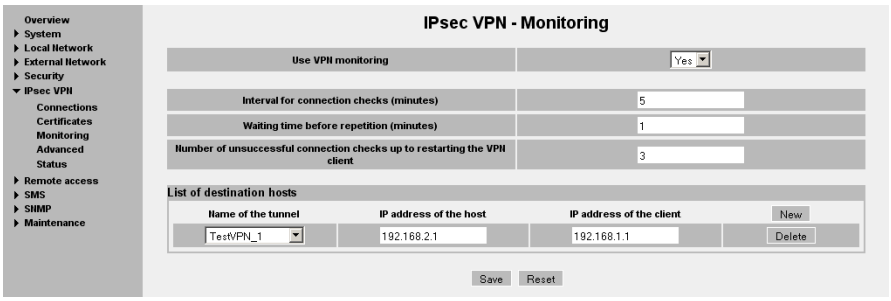
Protocol	**All**

From IP address	**0.0.0.0/0**
From port	**ANY**
To IP address	**0.0.0.0/0**
To port	**ANY**
Action	**Drop**
Log	**No (switched off)**
Log entries for unknown incoming connection attempts	**No (switched off)**
Log entries for unknown outgoing connection attempts	**No (switched off)**

7.6 Monitoring of VPN connections

IPsec VPN > Monitoring

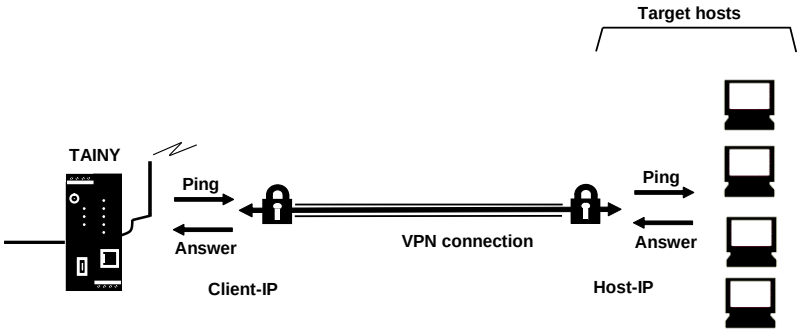
ONLY TAINY xMOD-V3



Function

With the supervision of VPN connections the TAINY xMOD-V3 checks the condition of configured VPN connections. To check the VPN connection status the TAINY xMOD-V3 sends periodically ping packets (ICMP) via the VPN connection to one or several remote stations (target hosts). This is made independently from payload data. For each VPN connection an own supervision can be configured.

If the TAINY xMOD-V3 receives the answer for the ping packet from at least one addressed remote station, the VPN connection is still operational.



If none of the receivers answers the ping, the following sequence takes place:

- Defined number of repetitions of the ping test
- Defined number of repetitions of the ping test with a re-established tunnel each time
- Restart of the VPN client

A requirement for this sequence is that the tunnel can be established, but the receiver used for the test is not reached. As soon as a ping test is successful, this sequence is discontinued. If the tunnel cannot be established, the sequence described in Chapter 7.7 is initiated due to failure to establish tunnel connections.

Warning

Sending the ping packages (ICMP) increases the amount of data sent and received over the mobile data service connection (HSPA+, UMTS, EGPRS or GPRS). Depending on the selected settings, the additional data traffic can amount to 4.5 Mbyte per month or more. This can lead to additional costs.

Note

The supervision of the VPN connections by ping partly overlaps the monitoring functions of Dead Peer Detection. Ping supervision activated can increase the DPD delay.

Use VPN monitoring

Yes VPN monitoring on

No VPN monitoring off

Interval for connection checks

This parameter determines the time interval to send ping packets through the supervised VPN connection (VPN tunnel).

The value shall be given in minutes.

Waiting time before repetition

This parameter determines the delay a ping packet is repeated after a failed ping check (ping packet not answered).

The value shall be given in minutes.

Number of unsuccessful connection checks up to restarting the VPN client

This parameter defines the number of ping test repetitions for two different stages in this sequence:

- Number of repetitions of the ping test until the first restart of the VPN connection
- Number of ping tests with corresponding restart of the tunnel connection or connections until the restart of the VPN client

List of destination hosts

Name of the tunnel Determine, which VPN connection (VPN tunnel) shall be supervised. Add a VPN connection by clicking the *New* button; delete a VPN connection by clicking the *Delete* button.

IP address of the host Enter the IP address of the remote station (target host) here.

IP address of the client Enter here any unused IP address of the local network related to the VPN connection.

Use *New* to add a destination host to the *List of destination hosts* and *Delete* to remove a host from the list.

Factory setting

The factory settings used by the TAINY xMOD-V3 are as follows:

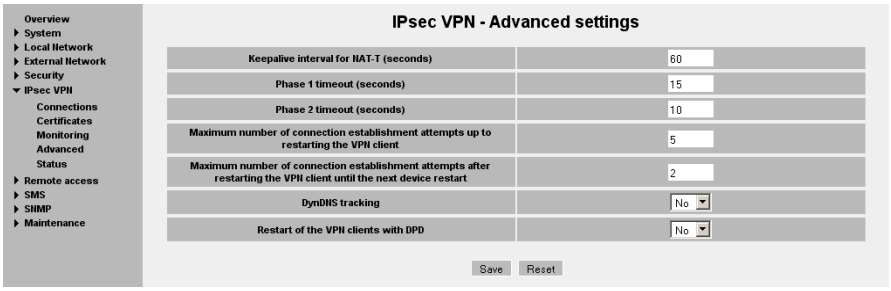
Use VPN monitoring	**No**
Interval for connection checks (minutes)	**5**
Waiting time before repetition (minutes)	**1**
Number of unsuccessful connection	**3**

checks up to restarting the VPN client	
Name of the tunnel	**-**
IP address of the host	**192.168.2.1**
IP address of the client	**192.168.1.1**

7.7 Advanced settings for IPsec VPN connections

IPsec VPN > Advanced Settings

ONLY TAINY xMOD-V3



Function	Setting special timeouts and intervals for VPN connections.
Keepalive interval for NAT-T (seconds)	If NAT-T is enabled (cf. Chapter 0), then keepalive data packets will be sent periodically by the TAINY xMOD-V3 through the VPN connection. The purpose of this is to prevent a NAT router between the TAINY xMOD-V3 and the remote station from interrupting the connection during idle periods without data traffic. Here you can change the interval between the keepalive data packets.
Phase 1 timeout (seconds)	The Phase 1 timeout determines how long the TAINY xMOD-V3 waits for completion of an authentication process of the ISAKMP-SA. If the set timeout is exceeded, the authentication will be aborted and restarted. Here you change the timeout.
Phase 2 timeout (seconds)	The Phase 2 timeout determines how long the TAINY xMOD-V3 waits for completion of an authentication process of the IPsec-SA. If the set timeout is exceeded, the authentication will be aborted and restarted. Here you change the timeout.
Maximum number of connection establishment attempts up to restarting the VPN client	If the establishment of a VPN connection fails, the connection setup will be retried by the TAINY xMOD-V3. Enter the number of unsuccessful retries, being performed before the TAINY xMOD-V3 restarts its VPN client before trying again the connection setup.
Maximum number of connection establishment attempts after restarting the VPN client until the next device restart	If the establishment of a VPN connection fails, the TAINY xMOD-V3 will retry to set up the connection. After a defined number of failed attempts the TAINY xMOD-V3 restarts its VPN client. Enter here the number of unsuccessful retries being performed after the VPN client has already been restarted and before the TAINY xMOD-V3 reboots and tries again to setup the connection.
DynDNS tracking	If the VPN gateway of the remote stations uses a DynDNS service to get an IP address and no Dead Peer Detection is used, the TAINY xMOD-V3 should periodically check if the remote VPN gateway is still reachable. The DynDNS tracking function provides this service. *Yes* activates this function, *No* deactivate this function.
Interval for DynDNS tracking (minutes)	Configure here the interval it shall be checked, if the remote station is still reachable.

Restart of the VPN clients on DPD	Here you can specify whether the VPN client should be restarted in the event of a Dead Peer Detection (DPD).

Factory setting

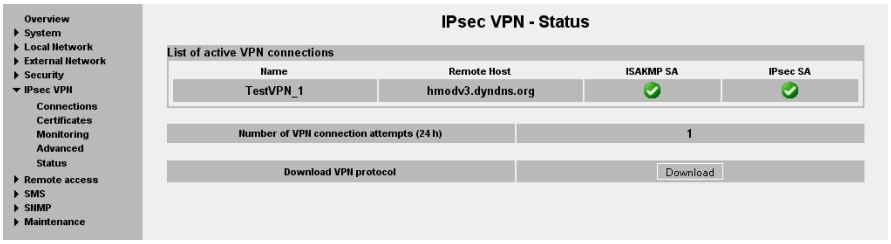
The factory settings used by the TAINY xMOD-V3 are as follows:

Keepalive interval for NAT-T (seconds)	**60**
Phase 1 timeout (seconds)	**15**
Phase 2 timeout (seconds)	**10**
Maximum number of connection establishment attempts up to restarting the VPN client	**5**
Maximum number of connection establishment attempts after restarting the VPN client until the next device restart	**2**
DynDNS tracking	**No**
Interval for DynDNS tracking (minutes)	**5**
Restart of the VPN clients on DPD	**No**

7.8 Status of the VPN connections

IPsec VPN > Status

ONLY TAINY xMOD-V3



Function	Indicates the status of the enabled VPN connections and the option for loading a protocol file to the Admin PC.
List of active VPN connections	The respective security association (SA) has been successfully established. The security association has not been established.
Number of VPN connection attempts (24h)	Shows the number of attempts to establish the activated VPN connections since 0:00 (system time)
Download VPN protocol	This function can be used to download the VPN protocol file to the Admin PC.

8 OpenVPN connection

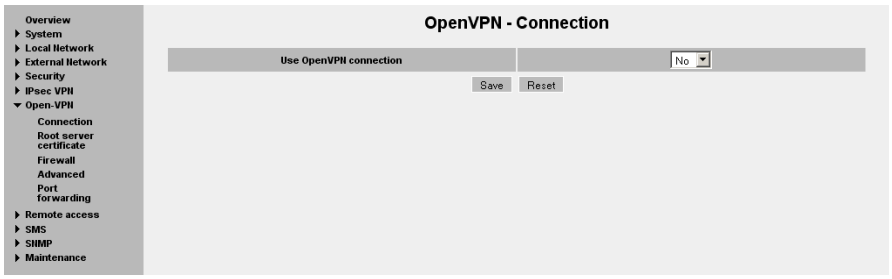
ONLY TAINY xMOD-V3

Note regarding the scope of function

The OpenVPN menu item is only available in TAINY xMOD-V3 devices. Only TAINY xMOD-V3 devices support OpenVPN connections.

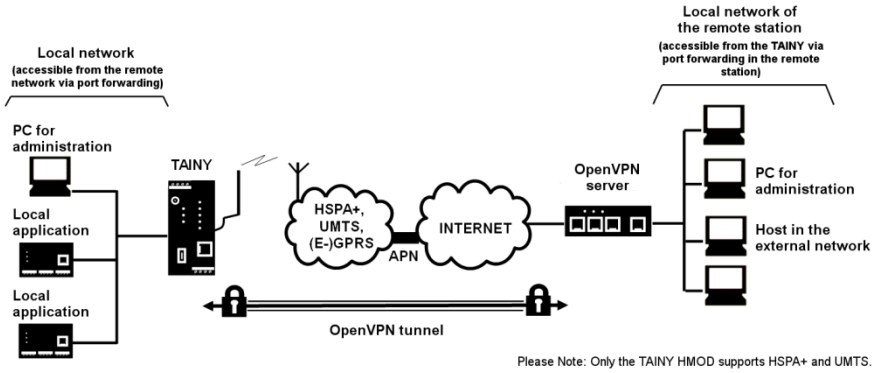
8.1 Introduction

ONLY TAINY xMOD-V3



Function

The TAINY xMOD-V3 can be connected to a remote OpenVPN server via OpenVPN. The IP data packets exchanged between the two OpenVPN end points are encrypted and protected by the OpenVPN tunnel against unauthorised manipulation. Therefore, unprotected public networks like the internet can be used for the transmission of data without endangering the confidentiality or integrity of the data.



The TAINY xMOD-V3 works exclusively as an OpenVPN client that initiates the connection to an OpenVPN server. Therefore, the opposite endpoint has an OpenVPN server which accepts the connection.

Note

The implementation of OpenVPN is restricted to the use of username and password in combination with a root server certificate. Other methods of authentication are currently not supported.

For authentication at the OpenVPN server the TAINY xMOD-V3 requires the following information, which you normally receive from the administrator of the OpenVPN server.

- permanent IP address or domain name of the OpenVPN server
- Port through which the OpenVPN connection should be established
- User name and password for login to the OpenVPN server
- Root server certificate (root certificate) of the OpenVPN server

Unlike with IPsec VPN, the TAINY xMOD-V3 only supports one OpenVPN

connection.

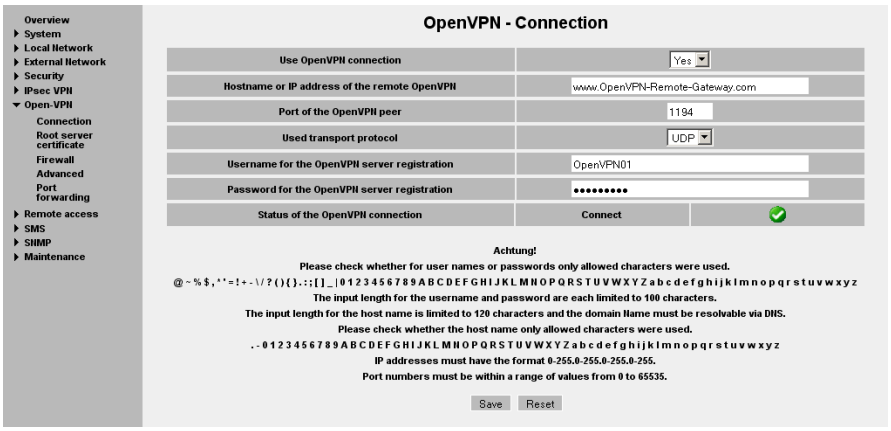
The TAINY xMOD-V3 authenticates itself with the OpenVPN server through the user name/password combination received from the administrator of the OpenVPN server. With successful authentication the OpenVPN client of the TAINY receives its own IP address.

For the authentication of the OpenVPN server at the TAINY xMOD-V3, the root server certificate of the OpenVPN server must be installed in the TAINY xMOD-V3.

8.2 Connection settings

OpenVPN > Connection

ONLY TAINY xMOD-V3



Function	Set up the TAINY xMOD-V3 according to the instructions of the system administrator of the remote location.
Use OpenVPN connection	Here you activate the OpenVPN function of the TAINY xMOD-V3: With *Use OpenVPN connection – Yes* you switch on the OpenVPN function of the TAINY xMOD-V3; with *No* it is switched off. After activation of the OpenVPN function, input fields for the configuration of the OpenVPN connection are shown.
Hostname or IP address of the remote OpenVPN Gateway	Enter the address of the remote location here, either as a host name (e.g. myadress.com) or as an IP address.
Port of the OpenVPN peer	Here you specify the port through which the OpenVPN connection should be established and operated.
Used transport protocol	Here you specify the protocol through which the OpenVPN connection should be established and operated. OpenVPN can use *TCP* or *UDP*.
Username for the OpenVPN server registration	Here you enter the user name with which the TAINY xMOD-V3 should log in to the OpenVPN server.
Password for the OpenVPN server registration	Enter the password with which the TAINY xMOD-V3 should log in to the OpenVPN server in combination with the user name.
Enable 1-to-1 NAT	The TAINY xMOD-V3 has a 1-to-1-NAT function with the opposing network of the OpenVPN connection.

The following information must be known for this (to be obtained from the wireless service provider or contract partner):

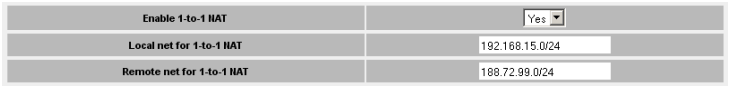
- the IP address of the remote network and the
- network mask of the remote network

If 1-to-1 NAT is switched off, local applications must use this address range for the addressing of remote locations in the remote network of the OpenVPN connection.

If 1-to-1 NAT is activated, a locally used address range can be defined through which the local applications can address the remote locations in the remote network of the OpenVPN connection.

The 1-to-1 NAT function in TAINY xMOD-V3 then maps the locally defined address range of the remote network (*Local net for 1-to-1 NAT*) on the actual address range of the remote network (*Remote net for 1-to-1 NAT*) of the OpenVPN connection.

No	The TAINY xMOD-V3 does not use 1-to-1-NAT for the remote network of the OpenVPN connection.
Yes	The TAINY xMOD-V3 uses 1-to-1-NAT for the remote network of the OpenVPN connection.



Local net for 1-to-1 NAT

Enter the IP address here complete with network mask, via which the remote network of the OpenVPN connection is to be accessed from the local network of the TAINY xMOD-V3. Use the CIDR format for this (see Section 16). Example: 192.168.15.0/24.

Remote net for 1-to-1 NAT

Enter the actual address of the remote network of the OpenVPN connection here. You can obtain this information from your wireless network operator or contract partner. Enter the address in CIDR format (see Section 16). Example: 188.72.99.0/24.

Status of the OpenVPN connection

In *Status of the OpenVPN connection* the respective status of the OpenVPN connection is shown. There are the following statuses:

Init	The OpenVPN service is being initialised.
WAN Waiting	The TAINY has not yet received an IP address from the external network. OpenVPN still cannot establish a connection.
Configuring	The configuration for the OpenVPN connection is read, tested and loaded from the configuration file.
Connecting	The TAINY is currently attempting to establish an OpenVPN connection.
Connect	The OpenVPN connection has been successfully established.
Delaying	The TAINY is experiencing problems establishing the OpenVPN connection and the time interval defined under *Waiting time between connection attempts to the remote site* has begun (see also 8.5).

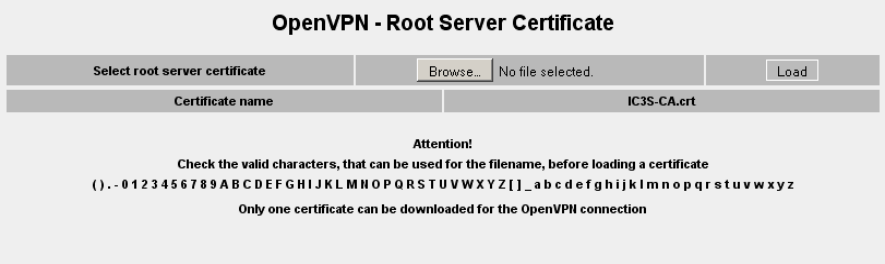
In addition to the status text, the symbol shows whether an OpenVPN connection has been established:

	The OpenVPN connection has been successfully established.
	No OpenVPN connection has been established

8.3 Root server certificate

OpenVPN > Root Server Certificate

ONLY TAINY xMOD-V3



Function

In order to check the authenticity of the selected OpenVPN server, the TAINY xMOD-V3 requires a copy of the root server certificate stored in the OpenVPN server. This copy must be installed in the TAINY xMOD-V3 before the initial connection is established.

Select root server certificate

Here you select the required root server certificate for connection to the OpenVPN server and install it on the TAINY xMOD-V3 with *Load*.

Certificate name

After the successful installation of the root server certificate, its name is shown here.

Note

Only one root server certificate can currently be stored in the device.

Note

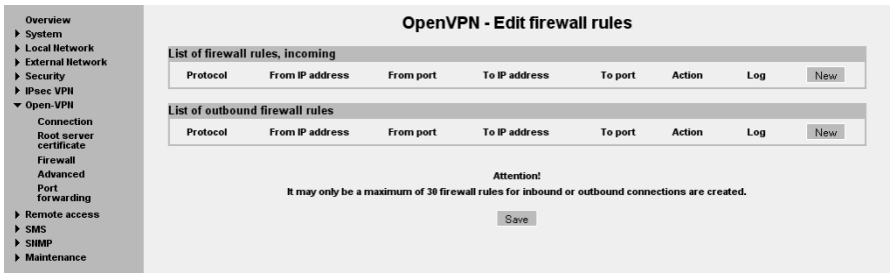
Root server certificates can be overwritten, but not deleted. To overwrite, select a new certificate and install it in the device. The previous certificate is replaced in the process.

8.4 Firewall rules for the OpenVPN connection

OpenVPN > Firewall

ONLY TAINY xMOD-V3

Under *OpenVPN* > *Firewall,* firewall rules can be set up for the OpenVPN connection:



OpenVPN – Edit Firewall Rules

The factory settings block data traffic through the OpenVPN tunnel. However, you can enable targeted data traffic by establishing corresponding firewall rules.

Proceed with the setup of the firewall rules for the OpenVPN connection in the same manner as for the setup of the packet filter function of the general firewall (see chapter 6.1).

The rules defined here apply exclusively for the OpenVPN connection.

Factory setting

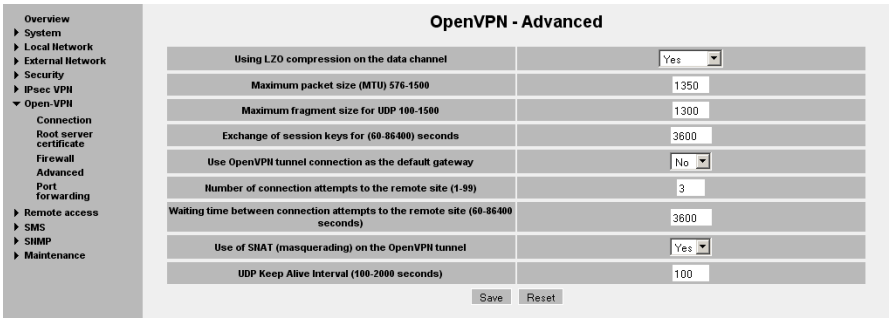
The factory settings used by the TAINY xMOD-V3 for a newly created firewall rule (incoming and outgoing) are as follows:

Protocol	**All**
From IP address	**0.0.0.0/0**
From port	**ANY**
To IP address	**0.0.0.0/0**
To port	**ANY**
Action	**Drop**
Log	**No**

8.5 Advanced settings for the OpenVPN connections

OpenVPN > Advanced

ONLY TAINY xMOD-V3



Function

Here you adjust the wait times, intervals, packet sizes and additional functions for the OpenVPN connection.

Enable LZO compression on the data channel

Here you specify whether the data on the OpenVPN connection should be compressed according to the LZO algorithm (Lempel Ziv Oberhumer algorithm).

With *Yes*, the LZO compression is enabled; with *No* it is disabled.

Maximum packet size/MTU

The *MTU* describes the maximum size of packets which can be sent over the OpenVPN connection. Larger packets must be internally divided into segments.

The maximum packet size (MTU) is variable from 576 to 1500 bytes.

Fragment UDP-Packets

Switch the fragmentation of UDP packets on or off here. The format of the UDP header is adapted depending on the setting.

No UDP packets are not fragmented and have no fragmentation bytes in the header.

Yes UDP packets may be fragmented and have four fragmentation bytes in the header.

Maximum fragment size for UDP

Determines the maximum size of UDP fragments after fragmentation.

The maximum fragment size is variable from 100 to 1500 bytes.

Exchange of session keys for

This parameter specified the time interval in which session keys of an existing OpenVPN connection are automatically renewed. Session keys are used for the encryption and decryption of data packets.

The time interval is variable from 60 s to 86400 s.

Use OpenVPN tunnel connection as the default gateway	If the OpenVPN tunnel connection is set as default gateway, all packets which are sent from the local network to IP addresses unknown to the TAINY are forwarded to the OpenVPN connection. With *Yes* the OpenVPN connection is set as the standard gateway; with *No* it is not.
Number of connection attempts to the remote peer	If the attempt at establishing connection to an OpenVPN server fails, the process is repeated according to the value specified here. Then the TAINY enters wait status before it begins again with the number of attempts specified here. The value range lies between 1 and 99 attempts.
Idle time between connection attempts to the remote peer	After the number of failed attempts parameterised above has been reached, the TAINY xMOD-V3 waits for the interval entered here (in seconds) before it attempts again to establish an OpenVPN connection. The valid value range for this parameter is 60 to 86400 s.
Use SNAT (masquerading) on the OpenVPN connection	With this parameter the SNAT (Source Network Address Translation) for OpenVPN connections can be activated (for more information about NAT, see also chapter 16) With *Yes*, Source NAT is activated; with *No* it is deactivated.
UDP Keepalive interval	The *UDP Keepalive interval* defines how long routing information of a known UDP connection is kept in the TAINY after the last packet was sent over the connection. The interval is restarted with each additional packet. It applies for all UDP routing information in the TAINY xMOD-V3. The time interval is variable from 100 s to 2000 s.

Factory setting

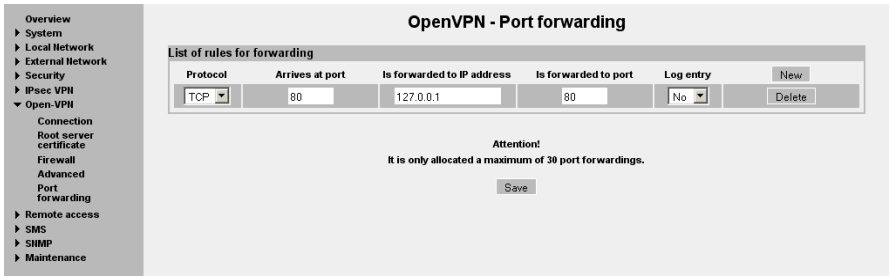
The factory settings used by the TAINY xMOD-V3 are as follows:

Enable LZO compression on the data channel	**Yes**
Maximum packet size/MTU	**1350**
Maximum fragment size for UDP	**1300**
Exchange of session keys for	**3600**
Use OpenVPN tunnel connection as the default gateway	**No**
Number of connection attempts to the remote peer	**3**
Idle time between connection attempts to the remote peer	**3600**
Use SNAT (masquerading) on the OpenVPN connection	**Yes**
UDP Keepalive interval	**180**

8.6 Port forwarding

OpenVPN > Port Forwarding

ONLY TAINY xMOD-V3



Function

If a corresponding rule for port forwarding is created here, data packets which arrive over the OpenVPN connection from the external network at a defined port of the TAINY xMOD-V3 are forwarded to a defined IP address and port number in the local network. The port forward can be configured for TCP or UDP.

The following takes place with port forwarding: The header of incoming data packets from the external network, which are directed over the OpenVPN connection to the IP address of the OpenVPN endpoint of the TAINY xMOD-V3 as well as a specific port, are rewritten so that they are forwarded to the internal network to a specific computer and a specific port of this computer. That means the IP address and port number in the header of incoming data packets are changed.

This process is called destination NAT or port forwarding.

Note

In order to be able to forward data packages arriving over the OpenVPN connection to the specified IP address in the local network, a corresponding incoming firewall rule must be set up for these IP addresses in the OpenVPN firewall (see chapter 8.4.).

New	Adds a new rule for forwarding that you can then fill out.
Delete	Removes rules for forwarding that have been created.
Protocol	Specify here the protocol (TCP or UDP) to which the rule should refer.
Arrives at port	Specify here the port number (e.g. 80) at which the data packets which are to be forwarded arrive from the external network.
Is forwarded to IP address	Specify here the IP address in the local network to which the incoming data packets should be forwarded.
Is forwarded to port	Specify here the port number (e.g. 80) for the IP address in the local network to which the incoming data packets should be forwarded.
Log entry	For each port forwarding rule you can define whether the event should be □ logged when the rule takes effect - set *Log entry* to *Yes* □ or not - set *Log entry* to *No* (factory setting) The log is kept in the firewall log, see Chapter 6.5.

Use the *Save* button to write parameter changes to the device‘s configuration

Factory setting

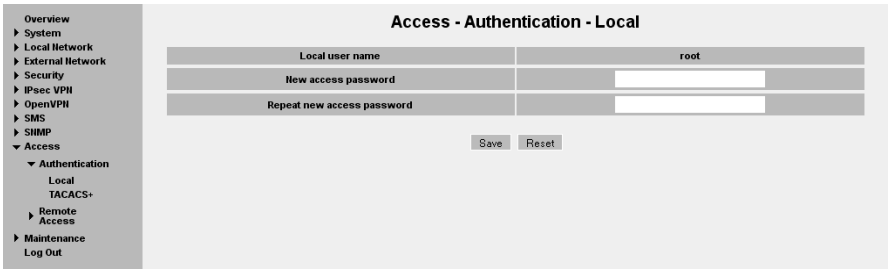
The factory settings for the TAINY xMOD are as follows:

List of rules for forwarding	**-**
Protocol	**TCP**
Arrives at port	**80**
Is forwarded to IP address	**127.0.0.1**
Is forwarded to port	**80**
Log entry	**No (switched off)**

9 Access

9.1 Authentication - Local

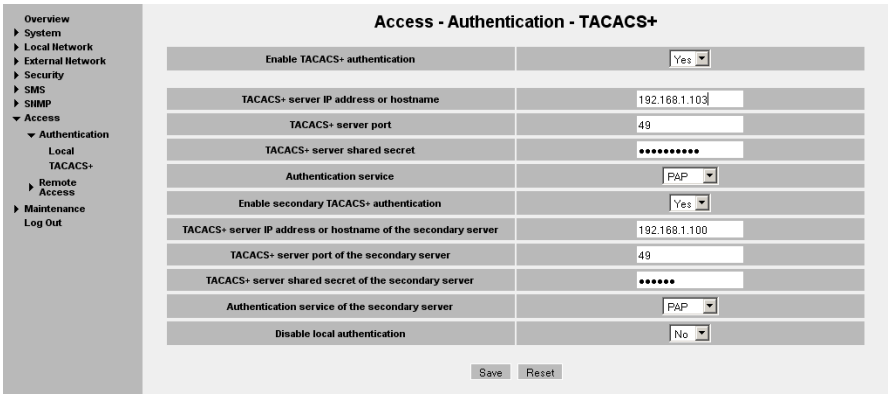
Access > Authentication > Local



The changing of the *access password* is described in chapter 3.9.

9.2 Authentication - TACACS+

Access > Authentication > TACACS+



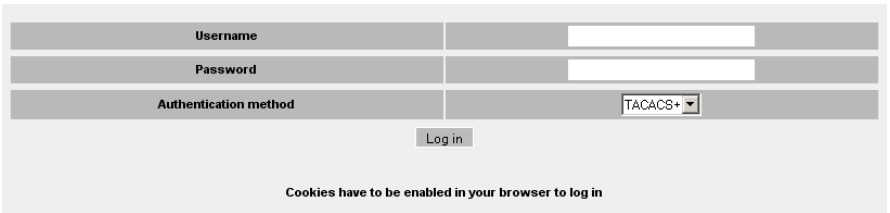
Function

With the authentication method TACACS+ (Terminal Access Controller Access Control System Plus), the access data for the TAINY xMOD are not saved in the device itself, but rather on an external server.

In the event of a registration request, the TAINY xMOD forwards the registration data to the TACACS+ server. The server checks the validity of the data and reports the result back to the TAINY xMOD, which then either rejects or accepts the registration.

Activate the authentication process TACACS+ here and set the parameters, which the TAINY xMOD needs for a connection to the TACACS+ server.

As soon as the TACACS+ service has been activated, the type of registration can be selected in the registration window (start screen) of the TAINY via an additional drop-down list (*TACACS+* or *Local*).



Note

Users who register on the TAINY xMOD via TACACS+ have no access to configuration pages where access rights can be changed:

- Access > Authentication > Local
- Maintenance > Execute Command
- Maintenance > Factory Reset

These websites are only available to locally registered users.

Enable TACACS+ authentication

Activate or deactivate the authentication via TACACS+ here:

No — The TACACS+ authentication is deactivated, i.e. registration on the TAINY xMOD can only take place *locally*.

Yes — The TACACS+ authentication is activated, i.e. registration on the TAINY xMOD can take place both *locally* and via TACACS+. Following activation, further input fields are shown, via which the data for registration on the TACACS+ server can be configured.

Enable secondary TACACS+ authentication

This parameter enables a secondary TACACS+ server, which is used by the TAINY xMOD for authentication if the primary TACACS+ server is not reachable or the use fails for another reason.

No — The use of a secondary TACACS+ server is deactivated, meaning the TAINY xMOD is using only the primary one. The input fields for the secondary TACACS+ server are hidden.

Yes — The usage of a secondary TACACS+ server is activated. input fields become visible which need to be filled to configure the parameter to access the secondary TACACS+ server. You can use the same parameter as for the primary one.

TACACS+ server IP address or host name (primary / secondary server)

Enter the address of the primary or secondary TACACS+ server here, either as a host name (e.g. myaddress.com) or as an IP address.

TACACS+ server port (primary / secondary server)

The port is entered here, via which the registration requests on the primary or secondary TACACS+ server have to be sent.

Shared secret (primary / secondary server)

This parameter contains a secret password, which is used to encrypt the data transfer to the primary or secondary TACACS+ server. It must match the password saved in the TACACS+ server.

Authentication service (primary / secondary server)

This parameter defines the authentication protocol, which is used during the TACACS+ registration. There are three protocols to choose from:

PAP — The registration is carried out via PAP (**P**assword **A**uthentication **P**rotocol).

CHAP — The registration is carried out via CHAP (**C**hallenge **H**andshake **A**uthentication **P**rotocol).

LOGIN — The registration takes place via an unencrypted terminal connection.

Disable Local

Deactivate the option to log-in by direct local authentication on the device.

Authentication

No — The log-in on TAINY xMOD is possible using a TACACS+ server as well as using log-in credentials stored directly inside the TAINY xMOD.

Yes — The log-in on TAINY xMOD is only possible using a TACACS+ server. Each SSH access is disabled also.

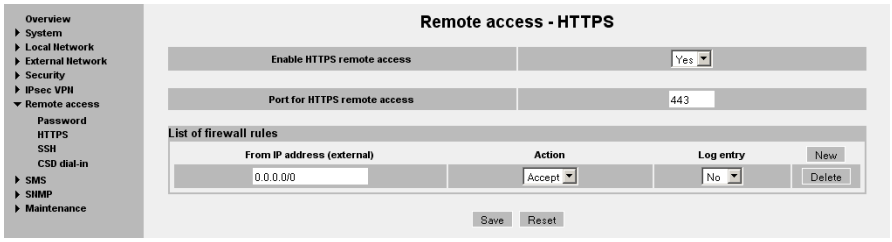
Factory settings

The factory settings for the TAINY xMOD are as follows:

Enable TACACS+ authentication	**No (switched off)**
TACACS+ server IP address or host name (primary / secondary server)	**192.168.1.100**
TACACS+ server port (primary / secondary server)	**49**
Shared secret (primary / secondary server)	**secret** (hidden)
Authentication service (primary / secondary server)	**PAP**
Enable secondary TACACS+ authentication	**No**
Disable Local Authentication	**No**

9.3 Remote access - HTTPS

Access > Remote Access > HTTPS



Function

The HTTPS remote access (= *HyperText Transfer Protocol Secure*) allows secure access to the Web user interface of the TAINY xMOD from an external network via HSPA+, UMTS, EGPRS, GPRS or CSD.

Configuration of the TAINY xMOD via the HTTPS remote access then takes place exactly like configuration via a Web browser via the local interface.

Enable HTTPS remote access

Yes — Access to the Web user interface of the TAINY xMOD from the external network via HTTPS is allowed.

No — Access via HTTPS is not allowed.

Port for HTTPS remote access

Default: 443 (factory setting)

Here you can define an alternative port. However, if you like to use the alternative port, the external remote station conducting the remote access must specify the port number after the IP address when specifying the address.

Example:
If this TAINY xMOD can be accessed via the Internet using the address 192.144.112.5, and if port number 442 has been defined for the remote access, then the following must be specified in the Web browser at the external remote station:
https://192.144.112.5:442

Note

Additionally to the new selected port, the standard port 443 for https remote access keeps open.

List of firewall rules

New — Adds a new firewall rule for HTTPS remote access that you can then fill out.

Delete — Removes a firewall rule for HTTPS remote access that has been created.

From IP address (external) — Specify here the address(es) of the computer(s) for which remote access is allowed. You have the following options:

IP address or address range: **0.0.0.0/0** means all addresses. To specify a range, use the CIDR notation - see Chapter 16.

Action — Define how access to the specified HTTPS port will be handled:

Accept means that the data packets can go through.

Reject means that the data packets are rejected, and the sender receives a message about the rejection.

Drop means that the data packets are not allowed through. They are discarded without the sender receiving any information about where they went.

Log entry — For each individual firewall rule you can define whether the event should be

- logged when the rule takes effect - set *Log* to *Yes*,
- or not - set *Log* to *No* (factory setting).

The log is kept in the firewall log, see Chapter 6.5.

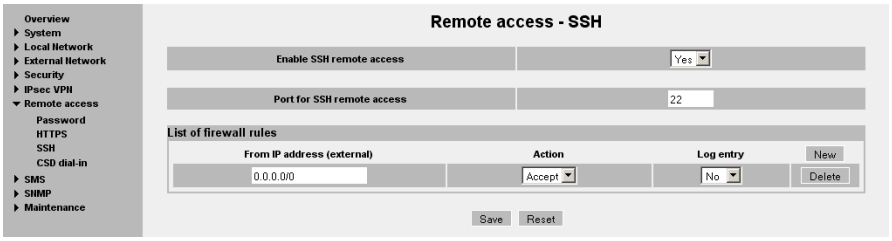
Factory setting

The factory settings for the TAINY xMOD are as follows:

Enable HTTPS remote access	**No (switched off)**
HTTPS remote access port	**443**
Default for new rules:	
From IP address (external)	**0.0.0.0/0**
Action	**Accept**
Log entry	**No (switched off)**

9.4 Remote access - SSH

Access > Remote Access > SSH



Function

The SSH remote access (= *Secured SHell*) allows secure access to the file system of the TAINY xMOD from an external network via HSPA+, UMTS, EGPRS, GPRS or CSD.

To do this, a connection must be established using an SSH-capable program from the external remote station to the TAINY xMOD.

Use the SSH remote access only if you are familiar with the LINUX file system.

In the factory setting this option is deactivated.

Warning

Via SSH remote access it is possible to derange the configuration of the device in such a way that it will have to be sent in for servicing. In this case please contact your dealer or distributor.

Warning

If the parameter *Disable Local Authentication* of the TACACS+ configuration is set to *Yes* the SSH access is disabled too (see 9.2).

Enable SSH remote access

Yes Access to the file system of the TAINY xMOD from the external network via SSH is allowed.

No Access via SSH is not allowed.

Port for SSH remote access

Default: 22 (factory setting)

You can define an alternative port. However, if you have defined an alternative port, then the external remote station conducting the remote access must specify the port number defined here in front of the IP address when specifying the address.

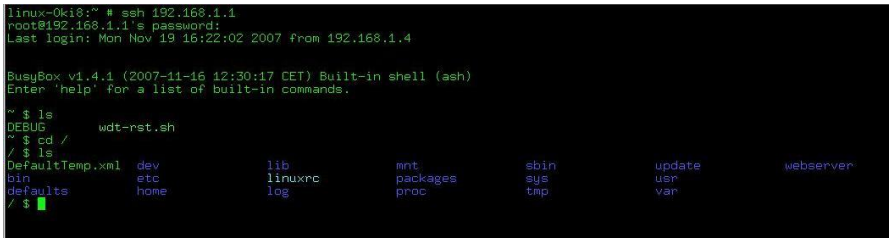
Note

Additionally to the new selected port, the standard port 22 for SSH remote access keeps open.

Example:
If this TAINY xMOD can be accessed from the external network using the address 192.144.112.5, and if port 22222 has been defined for the remote access, then this port number must be specified in the SSH client (e.g. PUTTY) at the external remote station:

SSH -p 22222 192.144.112.5

Example for console:



List of firewall rules

New Adds a new firewall rule for SSH remote access that you can then fill out.

Delete Removes a firewall rule for SSH remote access that has been created.

From IP address (external) Specify here the address(es) of the computer(s) for which remote access is allowed. You have the following options:

IP address or address range: **0.0.0.0/0** means all addresses. To specify a range, use the CIDR notation - see Chapter 16.

Action Define how access to the specified SSH port will be handled:

Accept means that the data packets can go through.

Reject means that the data packets are rejected, and the sender receives a message about the rejection.

Drop means that the data packets are not allowed through. They are discarded without the sender receiving any information about where they went.

Log entry For each individual firewall rule you can define whether the event should be

- logged when the rule takes effect - set *Log* to *Yes*,
- or not - set *Log* to *No* (factory setting).

The log is kept in the firewall log, see Chapter 6.5.

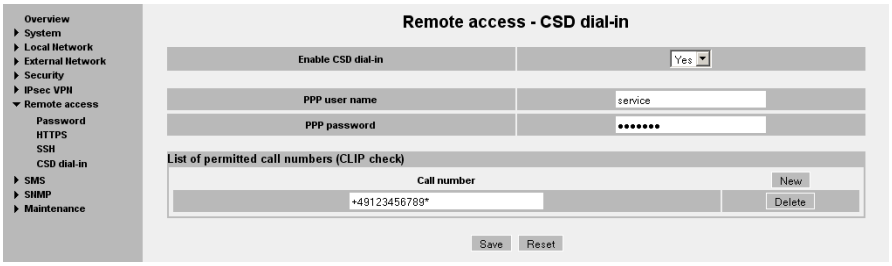
Factory setting

The factory settings for the TAINY xMOD are as follows:

Enable SSH remote access	**No (switched off)**
Port for SSH remote access	**22**
Default for new rules:	
From IP address (external)	**0.0.0.0/0**
Action	**Accept**
Log entry	**No (switched off)**

9.5 Remote access via dial-in connection

Access > Remote Access > CSD Dial-In



Function

The CSD dial-in access makes it possible to access the Web user interface of the TAINY xMOD via a dial-in data connection (*CSD* = *Circuit Switched Data*). To do this, call the TAINY xMOD at the data call number using an analogue modem, or at the voice or data call number of its SIM card using a GSM modem. The TAINY xMOD accepts the call if:

- the call number of the telephone connection that you call from is saved in the list of permitted numbers in TAINY xMOD, and
- the call number is transmitted by the telephone network (CLIP function)

Dialling must be performed by a PPP client, for example via a Windows dial-up connection. In Windows, use the *New Connection Wizard*, and under *Connect to the network at my workplace* set up a *Dial-up connection*.

Web interface and SSH console have the IP address 10.99.99.1. in case of CSD Dial-In.

ONLY FOR TAINY HMOD

Note

This function is available only, if a GSM network is used. In UMTS networks, this function cannot be used.

Enable CSD dial-in

Yes Access to the Web user interface of the TAINY xMOD from a dial-in data connection is allowed.

No Access via dial-in data connection is not allowed.

PPP user name / password

Select a user name and a password that must be used by a PPP client (e.g. a Windows dial-up connection) to log on to the TAINY xMOD. The same user name and the same password must be entered in the PPP client.

List of permitted call numbers (CLIP check)

Specify the call number of the telephone connection from which the dial-in data connection is established. The telephone connection must support Calling Line Identification Presentation (CLIP), and this function must be activated.

The call number entered in the TAINY xMOD must be exactly the same as the call number reported, and may also have to include the country code and prefix, e.g. +494012345678.

If multiple call numbers of a private branch exchange are to have access authorisation, you can use the "*" symbol as a wildcard, e.g. +49401234*. Then all call numbers that begin with +49401234 will be accepted.

Note

Firewall rules entered for HTTPS and SSH access also apply for CSD access. The source IP address (*"From IP"*) for CSD access is defined as 10.99.99.2.

New Adds a new approved call number for CSD remote access that you can then fill out.

Delete Removes a firewall rule for CSD remote access.

Factory setting

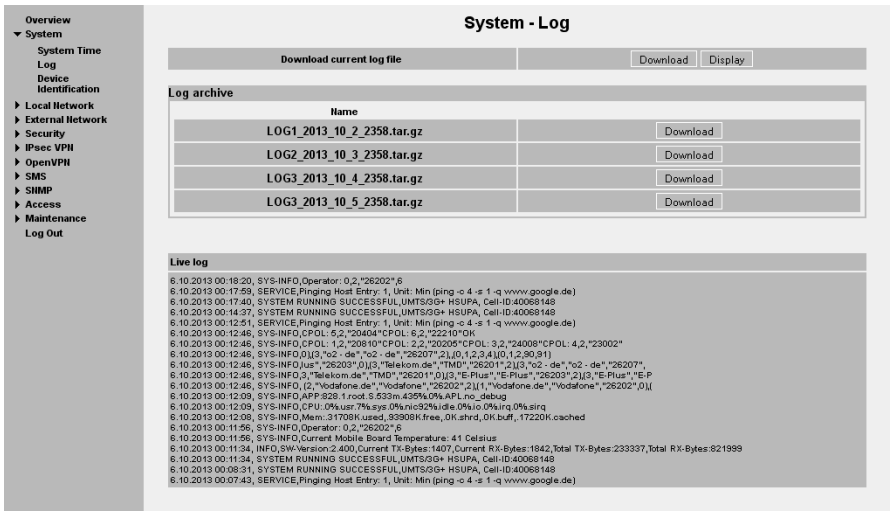
The factory settings for the TAINY xMOD are as follows:

Enable CSD dial-in	**No (switched off)**
PPP user name	**service**
PPP password	**service**
Call number	*****

10 Log, update and diagnosis

10.1 Log

System > Log



Log

Important events in the operation of the TAINY xMOD are saved in the log.

- Reboot
- Changes to the configuration
- Establishing of connections
- Interruption of connections
- Signal strength
- Memory and CPU load
- etc.

The log is saved to the log archive of the TAINY xMOD when a file size 1 Mbyte, is reached, but after 24 hours at the latest.

Download current logfile

Download - the current log is loaded to the Admin PC. You can select the directory to save the file to, and can view the file there.

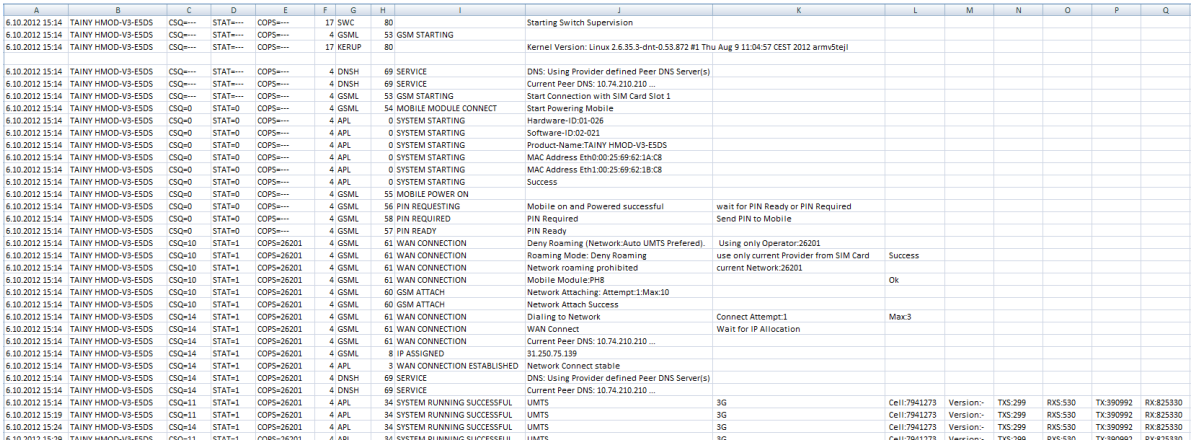
Log archive

Download - The archived log files are loaded to the Admin PC. You can select the directory to save the files to, and can view the files there.

Note

Unlike the current log, the log files for the log archive are available in a compressed format (*tar.gz). To view the log, open the compressed log file in a suitable extraction program and click through the folder structure. The actual log file has the file name *current.log*.

Example:



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=---	STAT=---	COPS=---	17	SWC	80		Starting Switch Supervision							
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=---	STAT=---	COPS=---	4	GSML	53	GSM STARTING								
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=---	STAT=---	COPS=---	17	KERUP	80		Kernel Version: Linux 2.6.35.3-dnt-0.53.872 #1 Thu Aug 9 11:04:57 CEST 2012 armv5tejl							
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=---	STAT=---	COPS=---	4	DNSH	69	SERVICE	DNS: Using Provider defined Peer DNS Server(s)							
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=---	STAT=---	COPS=---	4	DNSH	69	SERVICE	Current Peer DNS: 10.74.210.210 ...							
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=---	STAT=---	COPS=---	4	GSML	53	GSM STARTING	Start Connection with SIM Card Slot 1							
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=0	STAT=0	COPS=---	4	GSML	54	MOBILE MODULE CONNECT	Start Powering Mobile							
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=0	STAT=0	COPS=---	4	APL	0	SYSTEM STARTING	Hardware-ID:01-026							
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=0	STAT=0	COPS=---	4	APL	0	SYSTEM STARTING	Software-ID:02-021							
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=0	STAT=0	COPS=---	4	APL	0	SYSTEM STARTING	Product-Name:TAINY HMOD-V3-ESDS							
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=0	STAT=0	COPS=---	4	APL	0	SYSTEM STARTING	MAC Address Eth0:00:25:69:62:1A:C8							
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=0	STAT=0	COPS=---	4	APL	0	SYSTEM STARTING	MAC Address Eth1:00:25:69:62:1B:C8							
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=0	STAT=0	COPS=---	4	APL	0	SYSTEM STARTING	Success							
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=0	STAT=0	COPS=---	4	GSML	55	MOBILE POWER ON								
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=0	STAT=0	COPS=---	4	GSML	56	PIN REQUESTING	Mobile on and Powered successful	wait for PIN Ready or PIN Required						
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=0	STAT=0	COPS=---	4	GSML	58	PIN REQUIRED	PIN Required	Send PIN to Mobile						
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=0	STAT=0	COPS=---	4	GSML	57	PIN READY	PIN Ready							
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=10	STAT=1	COPS=26201	4	GSML	61	WAN CONNECTION	Deny Roaming (Network:Auto UMTS Prefered).	Using only Operator:26201						
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=10	STAT=1	COPS=26201	4	GSML	61	WAN CONNECTION	Roaming Mode: Deny Roaming	use only current Provider from SIM Card	Success					
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=10	STAT=1	COPS=26201	4	GSML	61	WAN CONNECTION	Network roaming prohibited	current Network:26201						
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=10	STAT=1	COPS=26201	4	GSML	61	WAN CONNECTION	Mobile Module:PH8		Ok					
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=10	STAT=1	COPS=26201	4	GSML	60	GSM ATTACH	Network Attaching: Attempt:1:Max:10							
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=10	STAT=1	COPS=26201	4	GSML	60	GSM ATTACH	Network Attach Success							
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=14	STAT=1	COPS=26201	4	GSML	61	WAN CONNECTION	Dialing to Network	Connect Attempt:1	Max:3					
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=14	STAT=1	COPS=26201	4	GSML	61	WAN CONNECTION	WAN Connect	Wait for IP Allocation						
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=14	STAT=1	COPS=26201	4	GSML	61	WAN CONNECTION	Current Peer DNS: 10.74.210.210 ...							
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=14	STAT=1	COPS=26201	4	GSML	8	IP ASSIGNED	31.250.75.139							
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=14	STAT=1	COPS=26201	4	APL	3	WAN CONNECTION ESTABLISHED	Network Connect stable							
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=14	STAT=1	COPS=26201	4	DNSH	69	SERVICE	DNS: Using Provider defined Peer DNS Server(s)							
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=14	STAT=1	COPS=26201	4	DNSH	69	SERVICE	Current Peer DNS: 10.74.210.210 ...							
6.10.2012 15:14	TAINY HMOD-V3-ESDS	CSQ=11	STAT=1	COPS=26201	4	APL	34	SYSTEM RUNNING SUCCESSFUL	UMTS	3G	Cell:7941273	Version:-	TXS:299	RXS:530	TX:390992	RX:825330
6.10.2012 15:19	TAINY HMOD-V3-ESDS	CSQ=11	STAT=1	COPS=26201	4	APL	34	SYSTEM RUNNING SUCCESSFUL	UMTS	3G	Cell:7941273	Version:-	TXS:299	RXS:530	TX:390992	RX:825330
6.10.2012 15:24	TAINY HMOD-V3-ESDS	CSQ=14	STAT=1	COPS=26201	4	APL	34	SYSTEM RUNNING SUCCESSFUL	UMTS	3G	Cell:7941273	Version:-	TXS:299	RXS:530	TX:390992	RX:825330

Entries in log

Column A: Time stamp

Column B: Dr. Neuhaus product number

Column C: Signal quality (CSQ value)

Column D: GSM login status

STAT = --- = Function not activated yet

STAT = 1 = Logged in to home network

STAT = 2 = Not logged in; searching for network

STAT = 3 = Login rejected

STAT = 5 = Logged in to third-party network (roaming)

Column E: Indication of the network operator identification with the 3-digit country code (MCC) and the 2-3-digit network operator code (MNC).

Example: 26201 (262 = country code / 01 = network operator code)

Column F: Category of the log report (for customer service)

Column G: Internal source of the log report (for customer service)

Column H: Internal report number (for customer service)

Column I: Log report in plain text

Column J to Q: Additional information on the plain text report, such as:

- Cell ID (identification number of the active GSM cell)

- Software version

- TXS, RXS (IP packets transmitted in the current connection)

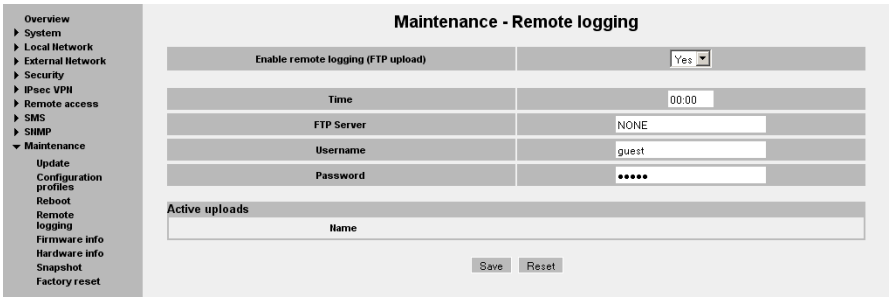
- TX, RX (IP packets transmitted since the last factory settings reboot)

Live log

The *Live Logbook* shows the most recent 20 logbook entries complete with time stamp. It updates automatically and provides a quick overview of the status and behaviour of the system.

10.2 Remote logging

Maintenance > Remote Logging



Function

The TAINY xMOD can transfer the system log once per day via FTP (= File Transfer Protocol) to an FTP server.

The current system log and the system log files in the archive are transferred. After a successful transfer the transferred logs are deleted in the TAINY xMOD.

If the transfer fails, the TAINY xMOD tries once again to transfer the data after 24 hours.

Note

After an unsuccessful FTP upload, the log files are stored under Maintenance > Remote Logging as *Active uploads*.

Enable remote logging (FTP upload)

Yes activates the function.

Time

Specifies the *Time* at which the logs are to be transferred.

FTP Server

Specifies the address of the *FTP server* to which the log files are to be transferred. The address can be specified as a host name (e.g. ftp.server.de) or as an IP address.

User name

Specifies the user name for logging in to the FTP server.

Password

Specifies the password for logging in to the FTP server.

Active uploads

If an FTP upload fails, those logfiles unsuccessfully sent will be moved from System > Log to the *Active uploads* list here. These files will be resent with the next attempt to upload via FTP.

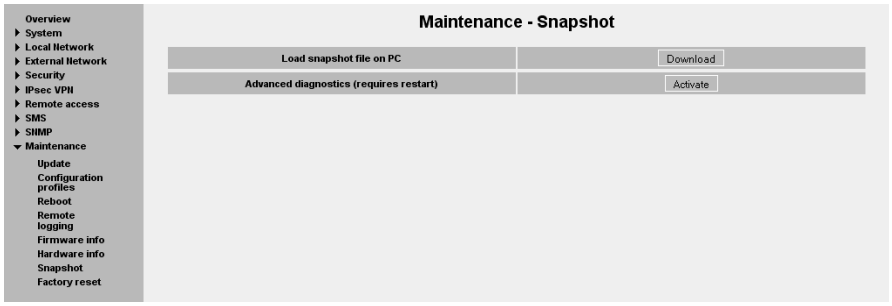
Factory setting

The factory settings for the TAINY xMOD are as follows:

Enable remote logging (FTP upload)	**No (switched off)**
Time	**00:00**
FTP Server	**NONE**
User name	**guest**
Password	**guest**

10.3 Snapshot

Maintenance > Snapshot



Function

This function is used for support purposes.

The service snapshot downloads important log files and current device settings that could be important for fault diagnosis and saves them in a file.

If you contact our customer service in the event of a problem with the TAINY xMOD, in many cases they will ask you for the snapshot file.

Note

This file contains the access parameters UMTS/GPRS and the addresses of the remote station. It does not contain the user name and password for access to the TAINY xMOD.

Load snapshot file on PC

Click on *Download*. You can select the location on the Admin PC where the snapshot file will be saved.

The filename of the snapshot file has the following structure:

<host name>_Snapshot_<Date&TimeCode>.tgz,

e.g.: tainyHMOD_Snapshot_200711252237.tgz

Advanced diagnosis (requires restart)

Please only *Activate* the *Advanced diagnosis* if asked to do so by our customer service. In operation with advanced diagnosis, information is written to the diagnosis logs much more often. Some additional information is also saved. This is useful for systematic troubleshooting.

On activation of *Advanced diagnosis* the TAINY xMOD will restart automatically

Note

When advanced diagnosis is active, the frequent write access to the non-volatile memory of the TAINY xMOD can lead to a reduction of its service life.

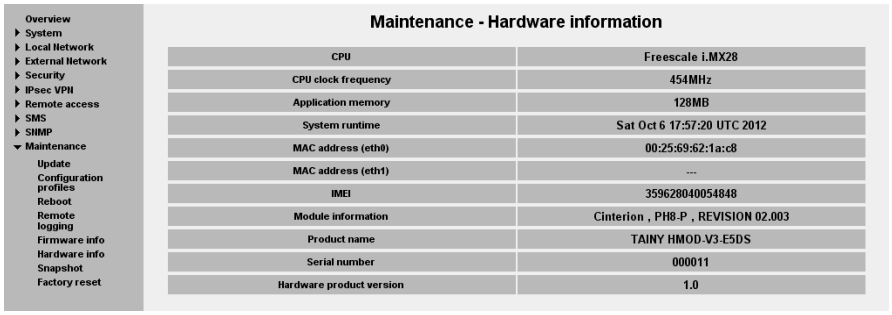
Factory setting

The factory settings for the TAINY xMOD are as follows:

Advanced diagnosis (requires restart) **Off (Activate)**

10.4 Hardware information

Maintenance > Hardware Info

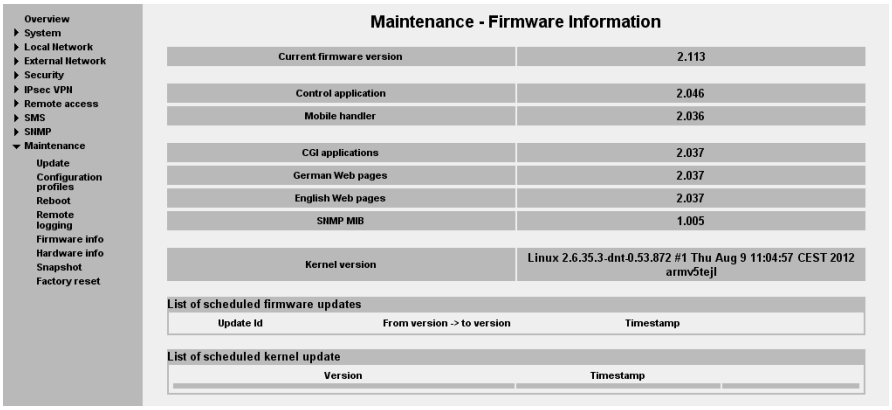


Function

Shows important information for hardware identification. This information is often needed in the event of queries to our customer service.

10.5 Firmware information

Maintenance > Firmware Info



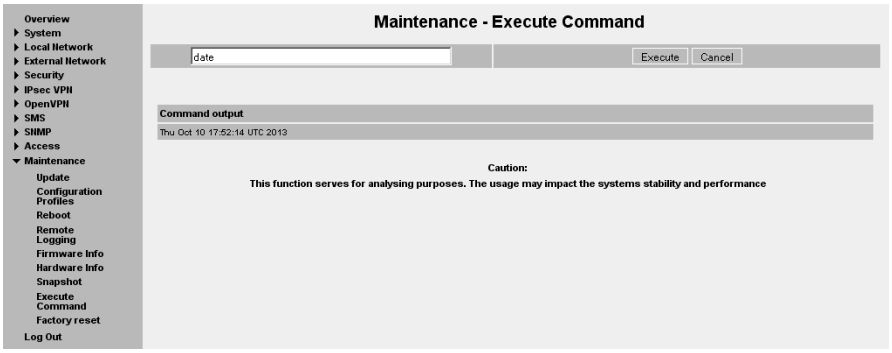
Function

Shows important information for software identification. This information is often needed in the event of queries to our customer service.

Planned firmware and kernel updates are also shown. See also Chapter 10.6

10.6 Execute command

Maintenance > Execute Command



Function

The *Execute command* function enables Linux command line commands to be sent to the TAINY. The TAINY executes the command directly and shows the results under *Command output*.

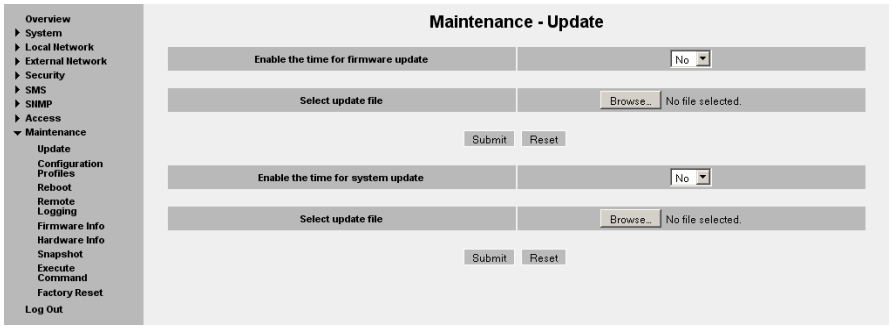
Caution

This function should only be used for problem analysis. Careless use can reduce the stability and performance of the system. It is possible to configure the device so incorrectly with Linux commands that it has to be sent in to service. In this case, please contact your dealer or distributor.

Execute	The entered command is sent to the TAINY.
Cancel	The command input field and *Command output* are deleted.

10.7 Firmware and system update

Maintenance > Update



Function

You can use the update function to load a new operating software (firmware) or a new system (kernel and driver) to the TAINY xMOD and activate these software components.

With an immediate update, the new software package (firmware or system) is first extracted. This process can take a few minutes. Then the actual update process begins, which is indicated by a chaser light of the LEDs ‘S’, ‘Q’ and ‘C’.

The settings of the TAINY xMOD are adopted, if they still work in the new software version as they did before the update.

Enable the time for firmware update

No	Immediate update - The new firmware is activated immediately after you load it and click on the *Submit* button.
Yes	Scheduled update - The new firmware is activated at a specified update time. For this purpose, the new firmware file must be loaded in advance.

Define the time for firmware update

If you wish to perform a time-controlled firmware update, enter the time at which the new firmware should be unpacked and activated.

Enter *Year – Month – Day – Hour – Minute*.

Select update file

Select the new firmware with *Browse*. For example, a firmware update file for the TAINY xMOD can have the following name:

EMOD_v2.008_v2.113.tgz

Load the firmware to the device with *Open*.

Submit

Submit starts the update process of the firmware, either immediately or at the specified time.

Reset

Reset clears *Select update file* for firmware updates and sets *Enable the time for firmware update* to *No*.

Enable the time for system update

No	Immediate update - The new kernel is activated immediately after you load it and click on the *Submit* button.
Yes	Scheduled update - The new kernel and driver of the system package are activated at a specified update time. For this

	purpose, the new kernel file must be loaded in advance.
Define the time for system update	If you wish to perform a time-controlled system update, enter the time at which the new kernel should be unpacked and activated. Enter *Year – Month – Day – Hour – Minute*.
Select update file	Select the new system update file with *Browse*. For example, a system update file for the TAINY xMOD can have the following name: - **tainy_system_package_update_all_1.0.tgz** Load the system update file to the device with *Open*.
Submit	*Submit* starts the update process of the system, either immediately or at the specified time.
Reset	*Reset* clears *Select update file* for system updates and sets *Enable the time for kernel update* to *No*.

11 SMS

11.1 Overview

The TAINY xMOD uses the Short Message Service (SMS) of GSM.

It is possible to define a specific SMS Center via Web user interface under *External Network - UMTS/EDGE* (TAINY HMOD) or *External Network - EDGE/GPRS* (TAINY EMOD), see chapter 5.1.

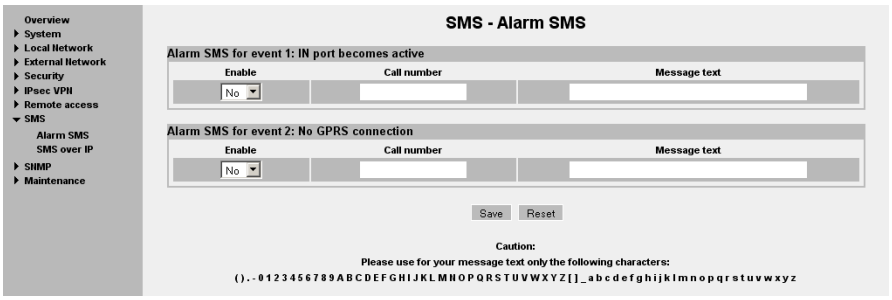
So that the SMS function will work reliably, enter the call number of the service center over there. Without any entry the default SMS service center of your network operator will be used.

Attention:

It is strongly recommended to enter a call number for the SMS center and use the international format (e.g. +49...) to ensure the SMS can be sent. Otherwise you may encounter problems.

11.2 Alarm SMS

SMS > Alarm SMS



Function

The TAINY xMOD can transmit short alarm messages via the SMS (= Short Message Service) of the GSM network. Two events can trigger transmission of an alarm message via SMS:

- Event 1: In port is activated
- Event 2: No UMTS/GPRS connection

A separate call number for sending the alarm message to can be specified for each of these two events. The text of the alarm message can also be freely defined.

Alarm SMS for event 1: IN port becomes active

Event 1: the In port switches from inactive to active, i.e. sufficient switching voltage is applied at the In port. This function can be used, for example to transmit alarm messages of the local applications outside of the IP data connections.

Alarm SMS for event 2: No GPRS Connection

Event 2: the UMTS/GPRS connection is not established despite multiple attempts. The TAINY xMOD then transmits an alarm message.

Settings

Enable	With *Yes* the alarm message is sent when the event occurs, with *No* it is not.
Call number	Here enter the call number of the end device to which the alarm message is to be sent via SMS. The end device must support SMS reception via GSM or fixed network.
Message Text	Here enter the text that should be sent as an alarm message. The following characters are supported: , * ' # % = <> ! & + - / ? ( ) . : ; 0 1 2 3 4 5 6 7 8 9 A B C D E

F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z (and Space)

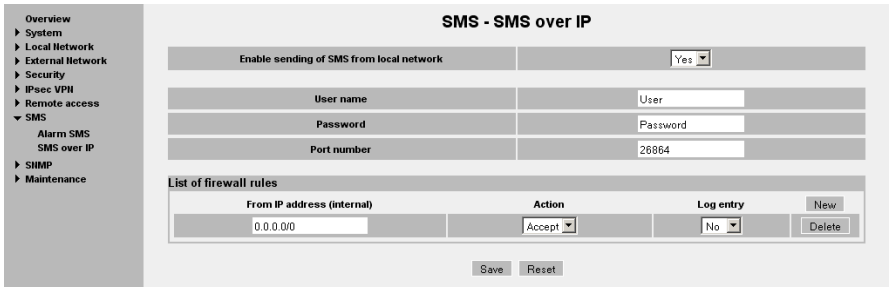
Factory setting

The factory settings for the TAINY xMOD are as follows:

Alarm SMS for event 1: IN port becomes active	
Enable	**No (switched off)**
Call number	**-**
Message Text	**-**
Alarm SMS for event 2: No GPRS connection	
Enable	**No (switched off)**
Call number	**-**
Message Text	**-**

11.3 SMS – SMS over IP

SMS > SMS over IP



Function

Applications being connected to the local interface of the TAINY xMOD can send messages to the TAINY xMOD which are forwarded then as Short Messages (SMS) via GSM.

To transmit an SMS the application at the local interface has to set-up a TCP/IP connection to the TAINY xMOD.

The application sends via the TCP/IP connection the text of the SMS to the TAINY xMOD. TAINY xMOD puts the text in a SMS and transmits it via GSM.

Framing over the TCP/IP connection

The text has to be send to the TAINY xMOD via the TCP/IP connection using the following frame format:

User name#Password#CommandCode#Seq-Num;Phonenumber;Text:

Example: user#password#105#01;0049043465789;MySMS Text:

User name

User name to check the right to send SMS. 10 characters maximum.

Password

Password to check the right to send SMS. 10 characters maximum.

CommandCode

Command to transmit SMS from the local network. This value is fixed to 105 and may not be changed.

Seq-Num

The sequence number is used to distinguish several SMS transmission jobs in parallel. The function is not supported yet.

The sequence number consists of 2 numeric characters between 01 and 99

Phone number

GSM telephone number of the SMS recipient. The GSM telephone number may not exceed 40 characters. International numbers (+49...) can be entered.

Text

SMS Text. The text may not exceed 160 characters. The supported characters are:

, * ' # % = <> ! & + - / ? ( ) . : ; 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z (and Space)

The following characters are reserved and may not appear in the SMS text (forbidden characters):

#	Separator of the first command level
;	Separator of the second command level
:	End of message indicator

Enable sending of SMS from local network

Click *Yes* to be able to send SMS from the local network. Click *No* to disable this function.

User name

User name, which has to be part of the message frame, which text shall be transmitted by SMS. 10 characters maximum.

Password

Password, which has to be part of the message frame, which text shall be transmitted by SMS. 10 characters maximum.

Port number

Number of the TCP/IP port at which the TAINY xMOD accepts the TCP/IP connection for SMS messaging.

Firewall Rules

A firewall rule has to be established to allow the TCP/IP connection for SMS messaging to the TAINY xMOD. Click *New* to enter several sources (From IP) for TCP/IP connections for SMS messaging. Click *Delete* to remove connections.

From IP address (internal)	Enter the IP address of the local application that is allowed to send IP packets to the external network. Do this by specifying the IP address or an IP range for the local application. 0.0.0.0/0 means all addresses. To specify a range, use the CIDR notation - see chapter 16.
Action	Define how SMS messaging over IP will be handled: *Accept* means that the data packets can go through. *Reject* means that the data packets are rejected, and the sender receives a message about the rejection. *Drop* means that the data packets are not allowed through. They are discarded without the sender receiving any information about where they went.

Log entry For each individual firewall rule you can define whether the event should be

- logged when the rule takes effect - set *Log* to *Yes*,
- or not - set *Log* to *No* (factory setting).

The log is kept in the firewall log, see Chapter 6.5.

Factory setting

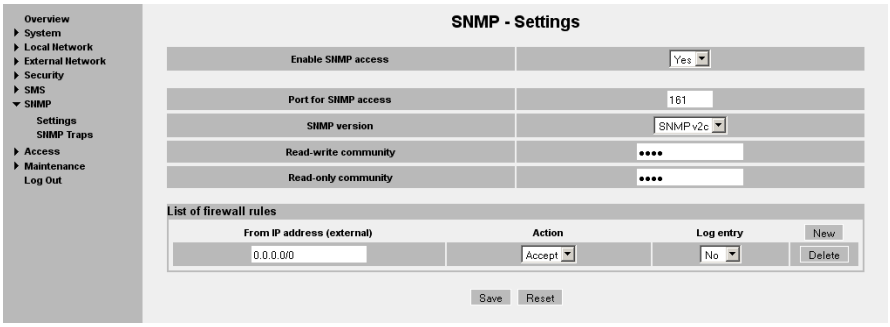
The factory settings for the TAINY xMOD are as follows:

Enable sending of SMS from local network	**No**
User name	**User**
Password	**Password**
Port number	**26864**
Firewall Rules	**Not active**
From IP address (internal)	**0.0.0.0/0**
Action	**Accept**
Log entry	**No**

12 SNMP

12.1 Operation via SNMP

SNMP > Settings



Various parameters of the TAINY xMOD can be queried or changed using SNMP (Simple Network Management Protocol) v2c or v3. SNMP v3 provides the most advanced security mechanism.

Access via SNMP can take place from both the local network and the external network.

The following SNMP queries and responses are supported by TAINY xMOD:

GET, GETNEXT, GETBULK, GETSUBTREE, WALK, SET, RESPONSE, TRAP.

The following parameters of the TAINY xMOD can be read via SNMP:

- Device identification lines (1-4)
- IP address of the external network
- PIN
- MAC address of the local interface
- Identification of the current wireless network operator
- APN
- IMSI
- IMEI
- Signal quality (CSQ value)
- Signal quality (dBm value)
- Net ID
- Cell ID
- Host name
- Maximum data volume
- Data volume of the 80 % warning threshold
- Data volume currently being used (monthly volume)
- Hardware ID
- Software version
- ICCID (Serial number of the SIM card in use)
- Access Technology (2G/3G)

The following parameters of the TAINY xMOD can be changed via SNMP:

- Maximum data volume (volume limit)
- PIN of the SIM card
- Device identification lines (1-4)

The exact description of the parameters is provided as a MIB (Management Information Base) on the Dr. Neuhaus website www.neuhaus.de. From there, go to the product page of the TAINY xMOD.

Enable SNMP access

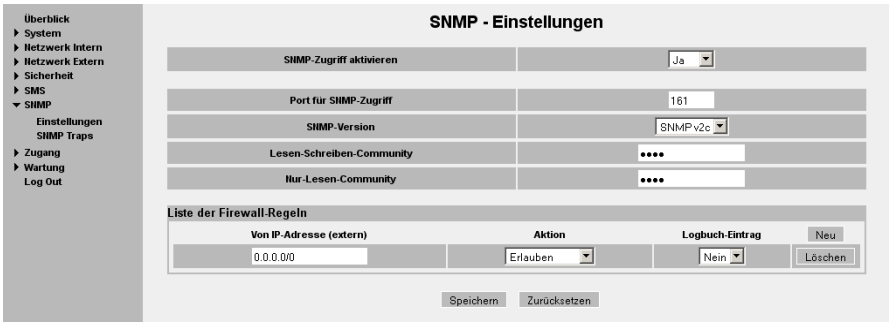
Select *No* if you want to block SNMP access to the TAINY xMOD.

Select *Yes* if you want to permit SNMP access to the TAINY xMOD.

Port for SNMP access

Select the IP port through which the SNMP access should take place. The factory setting is the standard (Port 161).

Using SNMP v2



Read-write community

Enter the SNMP community with reading and writing access rights to the TAINY xMOD.

Note

You should change the read-write community in any event. The factory setting ***private*** is general knowledge and does not provide sufficient protection.

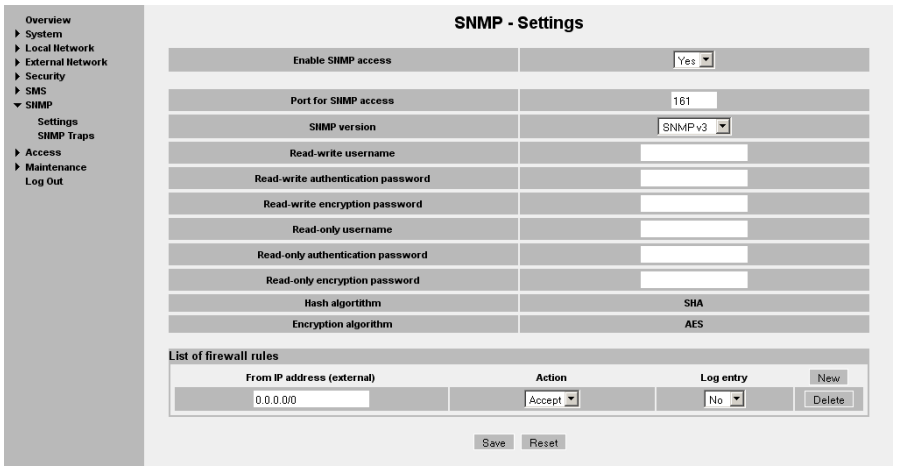
Read-only community

Enter the SNMP community with read-only access rights to the TAINY xMOD.

Note

You should change the read-only community in any event. The factory setting ***public*** is general knowledge and does not provide sufficient protection.

Using SNMP v3



Read-write username

Set the user name, which is used for authentication, if parameter of the

	TAINY xMOD may be written and read.
Read-write authentication password	Password which is used for authentication, if TAINY xMOD parameter may be read and written.
Read-write encryption password	Password which is used for encryption, if TAINY xMOD parameter may be read and written.
Read-only username	Set the user name, which is used for authentication, if parameter of the TAINY xMOD may be read-only.
Read-only authentication password	Enter the password which is used for authentication, if TAINY xMOD parameter may be read-only.
Read-only encryption password	Enter the Password which is used for encryption, if TAINY xMOD parameter may be read-only.
Hash algorithm	Indicates the used Hash-Algorithm. It cannot be changed.
Encryption algorithm	Indicates the used Encryption-Algorithm. It cannot be changed.
List of firewall rules	In order to be able to exchange data via SNMP, a firewall rule must be set upon the TAINY xMOD.

New	Sets up multiple sources (of IP) for the UDP/IP connection.
Delete	Removes the connections
From IP address (external)	Enter the IP address of the external remote location that may send IP packages to the local network. To do this, specify the IP address or an IP range of the remote location. 0.0.0.0/0 means all addresses. To specify a range, use the CIDR notation - see chapter 16.
Action	Select actions in order to enable the UDP/IP connection for SNMP. *Accept* means that the data packets can go through. *Reject* means that the data packets are rejected, and the sender receives a message about the rejection. *Drop* means that the data packets are not allowed through. They are discarded without the sender receiving any information about where they went.
Log entry	For each individual firewall rule you can define whether the event should be - logged when the rule takes effect - set *Log* to *Yes*, - or not - set *Log* to *No* (factory setting). The log is kept in the firewall log, see Chapter 6.5.

Factory setting

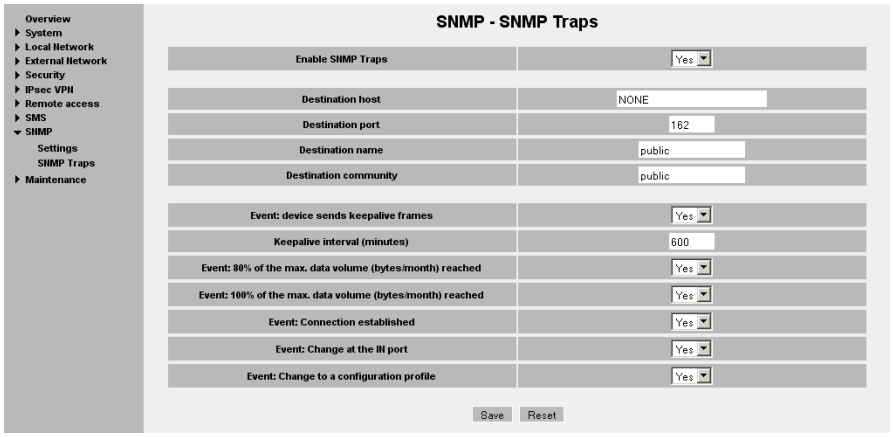
The TAINY xMOD has the following default settings:

Enable SNMP access	**No**
Port for SNMP access	**161**
Read-write community	**public**
Read-only community	**public**
Read-write username	(empty)
Read-write authentication password	(empty)

Read-write encryption password	(empty)
Read-only username	(empty)
Read-only authentication password	(empty)
Read-only encryption password	(empty)
Firewall rules	**Not active**
From IP address	**0.0.0.0/0**
Actions	**Accept**
Log entry	**No**

12.2 Alarm messages via SNMP traps

SNMP > SNMP Traps



The TAINY xMOD sends messages in the form of SNMP traps for various events.

Enable SNMP traps	Select *Yes* if you want to activate the sending of SNMP traps.
	Select *No* if you want to switch off the sending of SNMP traps.
Destination host	Enter the IP address of the SNMP trap recipient.
Destination port	Enter the IP port of the SNMP trap recipient.
Destination name	Enter the name of the SNMP trap recipient.
Destination community	Enter the name of the SNMP community here.
Event: device sends keepalive frames	Select *Yes* if you want the TAINY xMOD keepalive packages to be sent as an SNMP trap.
	Select *No* if you do not want the TAINY xMOD keepalive packages to not be sent as an SNMP trap.
Keepalive interval (minutes)	Choose the interval which you want the keepalive SNMP traps to be sent at.
Event: 80% of the max. data volume (bytes/month) reached	Select *Yes* if you want the TAINY xMOD to send an SNMP trap upon reaching the warning threshold (80 %) for the monthly data volume (see chapter 5.7).
	Select *No* if you do not want an SNMP trap to be sent for this event.
Event: 100% of the max. data volume	Select *Yes* if you want the TAINY xMOD to send an SNMP trap upon reaching the maximum monthly data volume (see chapter 5.7).

(bytes/month) reached	Select *No* if you do not want to set an SNMP trap for this event.
Event: Connection established	Select *Yes* if you want the TAINY xMOD to send an SNMP trap when successfully re-establishing the connection to the APN.
	Select *No* if you do not want to set an SNMP trap for this event.
Event: Change at the IN port	Select *Yes* if you want the TAINY xMOD to send an SNMP trap with a change at the switching input.
	Select *No* if you do not want an SNMP trap to be sent for this event.
Event: Change to a configuration profile	Select *Yes* if you want the TAINY xMOD to send an SNMP trap with the change of a configuration profile.
	Select *No* if you do not want an SNMP trap to be sent for this event.

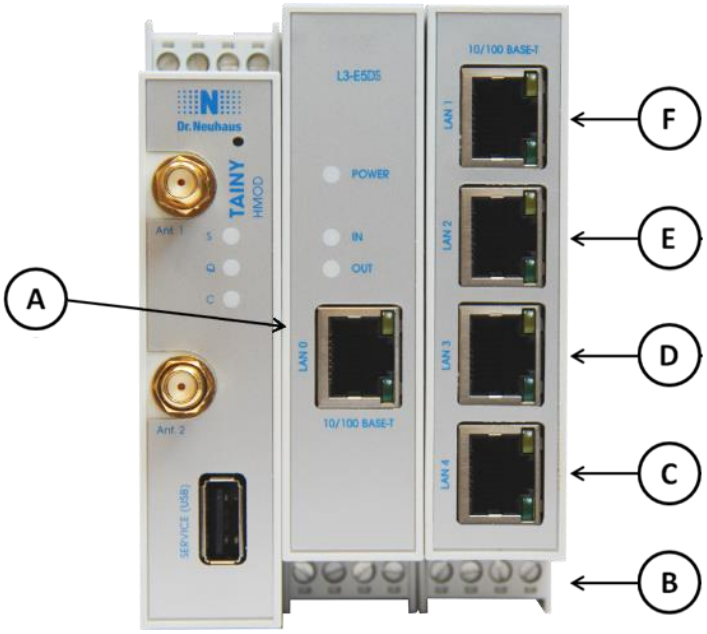
Factory setting

The TAINY xMOD has the following default settings:

Enable SNMP traps	No
Destination host	**NONE**
Destination port	**162**
Destination name	**public**
Destination community	**public**
Event: device sends keepalive frames	**Yes**
Keepalive interval (minutes)	**600**
Event: 80% of the max. data volume (bytes/month) reached	**Yes**
Event: 100% of the max. data volume (bytes/month) reached	**Yes**
Event: Connection established	**Yes**
Event: Change at the IN port	**Yes**
Event: Change to a configuration profile	**Yes**

13 Product version E5 (5 port Ethernet switch)

13.1 Overview



A – LAN0 / 10/100-Base-T RJ45 with integrated indicator lamps

B – 4 Connection terminals - Reserved for future applications

C – LAN4 / 10/100-Base-T RJ45 with integrated indicator lamps

D – LAN3 / 10/100-Base-T RJ45 with integrated indicator lamps

E - LAN2 / 10/100-Base-T RJ45 with integrated indicator lamps

F – LAN1 / 10/100-Base-T RJ45 with integrated indicator lamps

ONLY PRODUCT VERSION E5

The TAINY xMOD version E5 is equipped with a five port Ethernet switch.

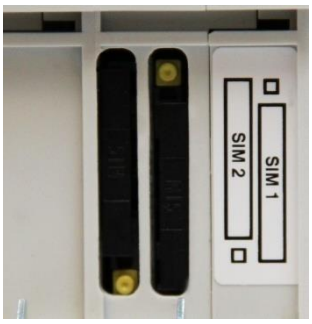
Function

All Ethernet ports are equivalent. They may be used to connect various applications or for the local configuration of the TAINY xMOD.

14 Product version DS (Dual SIM-Card)

14.1 Overview

ONLY PRODUCT VERSION DS



Function

TAINY xMODs version DS (Dual SIM-Card) are equipped with a second SIM card slot, which enables the device to establish a connection to the wireless data service (HSPA+, UMTS, EGPRS or GPRS) via another SIM card alternatively.

Example: the inserted SIM cards belong to different wireless data service providers. In case of the unavailability of one of the mobile networks the other provider's network can be used to establish a wireless data service connection and hence keep the application online.

Please note:

- SIM 2 is equivalent to SIM 1.
- Only one SIM card is enabled at a time.
- SIM cards are enabled by configuration profiles (or the configuration currently active). Each configuration profile is assigned to one SIM card slot only (see 5.1).
- Each SIM-card slot can be assigned to more than one profile
- The switching time between the SIM card slots depends largely on the dial-up times of the provider used. In the ideal scenario, a switch can be carried out in less than 50 seconds.

Use the Web user interface to determine which SIM card slot will be activated after a system reboot, i.e. which SIM card will be used to establish a wireless data service (HSPA+, UMTS, EGPRS or GPRS) connection per default.

Parameterization

For more information about the parameterization and switching of profiles, see chapter 15.

15 Profile change

15.1 Overview

Function

Different configurations can be stored in the TAINY xMOD as individual configuration profiles, and activated according to requirements.

In addition to manual profile activation, the device can be configured in such a way, that certain switching events lead to an automatic activation of a previously specified configuration profile.

For example this might be helpful if the connection to the network of the wireless data service (HSPA+, UMTS, EGPRS or GPRS) provider is unavailable. In this case it is possible to activate another profile containing an alternative APN (Access Point Name) setting or different access data for the provider.

ONLY PRODUCT VERSION DS

With TAINY xMOD with Dual SIM technology (product version DS) it is possible to enable a second SIM card slot, which provides the opportunity to use a completely different network operator in order to establish a wireless data service connection, if the network of the first provider fails.

Switching events

The changing of profiles can be triggered by four different switching events:

- Loss or unavailability of the wireless data service
- Connection check fails
- Reboot of the device
- Switching instant according to time-controlled schedule has been reached

15.2 Configuration

Below you will find an overview on where to configure profile changes for the respective profile switching events using the web user interface.

Please note:

Configuring profile changes, you can only select configuration profiles which have already been stored in the TAINY xMOD.

Switching event: Loss or unavailability of the wireless data service

Set the fallback profile for the switching event ‘loss or unavailability of the wireless data service’ here: parameter *At connection error fallback to profile* under *External network - UMTS/EDGE* (TAINY HMOD) or *External network - EDGE/GPRS* (TAINY EMOD) (see 5.1).

The setting ***NONE*** disables this function

Switching event: Connection check fails

Profile changes due to connection check failures require the following settings (under *External network - Advanced settings - Connection check)*:

- The connection check is enabled (Set *Enable connection check* to *Yes*)
- At least one host name is specified (*List of the ping targets*)
- *Activity on faulty connection* is set to *Activate another profile*

Use the parameter *To activate profile* to set the configuration profile that shall be activated in case of a connection check failure (see 5.2)

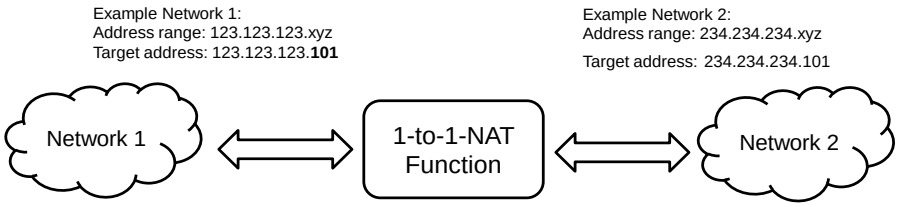
The setting ***NONE*** disables this function

Switching event: Reboot of the device	Set the initial profile after a system restart here: parameter *Initial profile after reboot* under *Maintenance - Configuration profiles* (see 3.8)
	Set to ***NONE*** there will be no profile change after a reboot. The device will start with the settings that were active before the reboot.
Switching event: Switching instant reached	Configure time-controlled switching events here: parameters *Change profile after (minutes)* and *to profile* under *Maintenance - Configuration Profiles* (see 3.8)
	Set to ***NONE*** this function is disabled.

16 Small lexicon of routers

1-to-1 NAT

With 1-to-1 NAT, a network component (e.g. router) maps the address range of one network to the address range of another network.



A component in Network 1 addresses a component in Network 2 through a target address from the address range of Network 1. The 1-to-1 NAT function maps the target address in the address range of Network 2. In turn, responses from Network 2 are received by a sender address from Network 1.

AES

Advanced Encryption Standard.

The NIST (National Institute of Standards and Technology) has developed the AES encryption standard in collaboration with industrial corporations for years. This → symmetric encryption should replace the previous DES standard. The AES standard specified three different key sizes with 128, 192 and 256 bit. In 1997 the NIST started an initiative for AES and revealed its conditions for the algorithm. From the proposed encryption algorithms the NIST narrowed the selection down to five algorithms: MARS, RC6, Rijndael, Serpent and Twofish. In October 2000 Rijndael was chosen as the encryption algorithm.

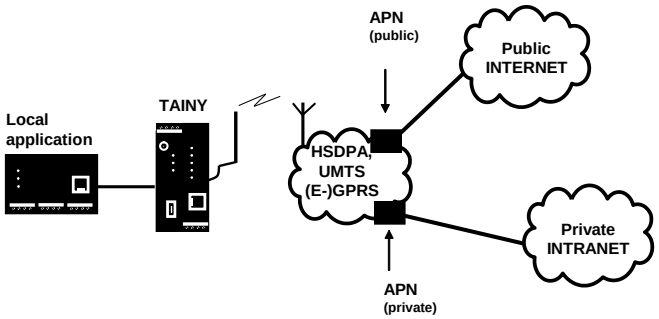
Antenna diversity

When antenna diversity is activated, an attempt is made with a second connected antenna to minimise faults and radio wave extinctions, which can occur due to reflections, different running times and overlapping. To this end, the signals from both antennas are evaluated and the signal deemed to be better is used.

In certain cases, it may be beneficial to operate the device with just one antenna in the direction of reception. The antenna diversity should be deactivated in this case.

APN (Access Point Name)

Trans-network connections, e.g. from a wireless network (HSPA+, UMTS, EGPRS or GPRS) to the Internet, are created in the wireless network via so-called APNs.



An end device that wants to establish a connection via the GPRS network specifies an APN to indicate which network it wants to be connected to: the Internet or a private company network that is connected via a dedicated line.

The APN designates the transfer point to the other network. It is communicated to the user by the network operator.

Asymmetric encryption

With asymmetric encryption, data is encrypted with a key and encrypted again with a second key. Both keys are suitable for encryption and decryption. One of the keys is kept secret by its owner (private key) and the other is given to the public (public key) - in other words, potential communication partners.

A message encrypted with the public key can only be decrypted and read by a recipient who has the corresponding private key. A message encrypted with the private key can only be decrypted and read by any recipient who has the corresponding public key. Encryption with the private key shows that the message actually originated from the owner of the corresponding public key. For that reason, the term “digital signature” is used.

However, asymmetric encryption processes such as RSA are slow and susceptible to certain types of attacks, which is why they are often combined with a symmetric process (→ symmetric encryption). On the other hand, concepts which eliminate the elaborate administrative efforts for symmetric keys are also possible.

CIDR

Classless Inter-Domain Routing

IP netmasks and CIDR are notations for grouping a number of IP addresses into an address space. Thus a range of contiguous addresses is treated as a network.

The CIDR method reduces, for example the routing tables stored in routers by means of a postfix in the IP address. This postfix can be used to designate a network together with its subnetworks. This method is described in RFC 1518.

In order to specify a range of IP addresses to the TAINY xMOD, or when configuring the firewall, it may be necessary to specify the address space in the CIDR notation. The following table shows the IP netmask on the left-hand side and to the far right the corresponding CIDR notation.

IP netmask	binary				CIDR
255.255.255.255	11111111	11111111	11111111	11111111	32
255.255.255.254	11111111	11111111	11111111	11111110	31
255.255.255.252	11111111	11111111	11111111	11111100	30
255.255.255.248	11111111	11111111	11111111	11111000	29
255.255.255.240	11111111	11111111	11111111	11110000	28
255.255.255.224	11111111	11111111	11111111	11100000	27
255.255.255.192	11111111	11111111	11111111	11000000	26
255.255.255.128	11111111	11111111	11111111	10000000	25
255.255.255.0	11111111	11111111	11111111	00000000	24
255.255.254.0	11111111	11111111	11111110	00000000	23
255.255.252.0	11111111	11111111	11111100	00000000	22
255.255.248.0	11111111	11111111	11111000	00000000	21
255.255.240.0	11111111	11111111	11110000	00000000	20
255.255.224.0	11111111	11111111	11100000	00000000	19
255.255.192.0	11111111	11111111	11000000	00000000	18
255.255.128.0	11111111	11111111	10000000	00000000	17
255.255.0.0	11111111	11111111	00000000	00000000	16
255.254.0.0	11111111	11111110	00000000	00000000	15
255.252.0.0	11111111	11111100	00000000	00000000	14
255.248.0.0	11111111	11111000	00000000	00000000	13
255.240.0.0	11111111	11110000	00000000	00000000	12
255.224.0.0	11111111	11100000	00000000	00000000	11
255.192.0.0	11111111	11000000	00000000	00000000	10
255.128.0.0	11111111	10000000	00000000	00000000	9
255.0.0.0	11111111	00000000	00000000	00000000	8

254.0.0.0	11111110	00000000	00000000	00000000	7
252.0.0.0	11111100	00000000	00000000	00000000	6
248.0.0.0	11111000	00000000	00000000	00000000	5
240.0.0.0	11110000	00000000	00000000	00000000	4
224.0.0.0	11100000	00000000	00000000	00000000	3
192.0.0.0	11000000	00000000	00000000	00000000	2
128.0.0.0	10000000	00000000	00000000	00000000	1
0.0.0.0	00000000	00000000	00000000	00000000	0

Example: 192.168.1.0 / 255.255.255.0 corresponds to CIDR: 192.168.1.0/24

Client / Server

In a client/server environment, a server is a program or computer that receives queries from a client program or client computer and answers them.

In data communication, a computer that establishes a connection to a server (or host) is also referred to as a client. That means that the client is the computer that is calling and the server (or host) is the one being called.

CSD 9600

CSD (9600) stands for Circuit Switched Data or dial-in data connection. Here a connection is created between two users (end points of the connection), similar to a telephone call over a public telephone network. User 1 dials the telephone number of user 2. The network signals to user 2 that there is a call, user 2 accepts the call and the network establishes the connection until one of the users terminates the connection again.

In a GSM network this service is called CSD, and allows data transmission at 9600 bit/s or 14400 bit/s, with transmission being either secured or unsecured. Possible connections are GSM modem to GSM modem, analogue modem to GSM and ISDN modem to GSM modem.

CSQ / RSSI

The CSQ value is a value defined in the GSM standard for indicating the signal quality. CSQ values correspond to the received field strength RSSI (= Received Signal Strength Indication):

	RSSI
< 6	< -101 dBm
6..10	-101 dBm.. - 93 dBm
11..18	- 91 dBm.. -77 dBm
> 18	> -75 dBm
99	Not logged in

Datagram

In the transmission protocol TCP/IP, data are sent in the form of data packets, the so-called IP datagrams. An IP datagram has the following structure:

1. IP Header
2. TCP/UDP Header
3. Data (Payload)

The IP Header contains:

- the IP address of the sender (source IP address)
- the IP address of the recipient (destination IP address)
- the protocol number of the protocol of the next higher protocol layer (according to the OSI layer model)
- the IP Header Checksum for checking the integrity of the header

upon receipt.

TCP/UDP Header contains the following information:

- the port of the sender (source port)
- the port of the recipient (destination port)
- a checksum for the TCP Header and a few items of information from the IP Header (source and destination IP addresses, etc.

DES / 3DES

The symmetric encryption algorithm (→ symmetric encryption) DES, originating from IBM and tested by the NSA, was established in 1977 by the American National Bureau of Standards, the predecessor to today's National Institute of Standards and Technology (NIST) as a standard for American governmental institutions. Since it was the first standardised encryption algorithm, it was also quickly adopted in industrial applications in the US and beyond.

DES works with a key length of 56bit, which can no longer be considered to be secure due to the increase in computing capability of the computer since 1977.

3DES is a variant of DES. It works with keys three times the size, which are 168 bits long. It is still considered to be secure and is also a part of the IPsec standard, among other things.

DHCP

The Dynamic Host Configuration Protocol (DHCP) performs automatic dynamic assignment of IP addresses and other parameters in a network. The Dynamic Host Configuration Protocol uses UDP. It was defined in RFC 2131 and was assigned the UDP ports 67 and 68. DHCP uses the client – server method, in which the client is assigned the IP addresses by the server.

DNS

Addressing in IP networks is always by means of IP addresses. It is generally preferable, however, to specify the addressing in the form of a domain address (i.e. in the form www.abc.xyz.de). If the addressing is by means of the domain address, then the sender first sends the domain address to a domain name server (DNS) and gets back the associated IP address. Only then does the sender address its data to this IP address.

DynDNS provider

Also *Dynamic DNS provider*. Every computer that is connected to the Internet has an IP address (IP = Internet Protocol). An IP address consists of up to 4 three-digit numbers, with dots separating each of the numbers. If the computer is online via the telephone line via modem, ISDN or ADSL, then the Internet service provider dynamically assigns it an IP address, i.e. the address changes from session to session. Even if the computer is online for more than 24 hours without interruption (e.g. in the case of a flat rate), the IP address is changed periodically.

For a local computer to be accessible via the Internet, its address must be known to the external remote station. This is necessary for it to establish a connection to the local computer. This is not possible, however, if the address of the local computer constantly changes. It is possible, however, if the user of the local computer has an account with a DynamicDNS provider (DNS = Domain Name Server).

Then he can specify there a host name, under which the computer can be accessed in the future, e.g.: www.xyz.abc.de. Moreover, the DynamicDNS provider makes available a small program that has to be installed and executed on the computer concerned. In each Internet session of the local computer this tool reports to the DynamicDNS provider which IP address the computer has at the moment. Its domain name server registers the current host name - IP address assignment and reports this to other domain name servers in the Internet.

If now an external computer wants to establish a connection with a local computer which is registered with the DynamicDNS provider, the external computer uses the host name of the local computer as the address. In this way a connection is established with the responsible DNS (Domain Name Server) in order to look up there the IP address which is currently assigned to this host name. The IP address is transmitted back to the external computer, and then used by it as the destination address. This now leads precisely to the desired local computer.

As a rule, all Internet addresses are based on this method: First a connection is established to a DNS in order to determine the IP addresses assigned to this host name. Once that has been done, the IP address that was "looked up" is used to establish the connection to the desired remote station, which can be any Web site.

EDGE

EDGE (= Enhanced Data Rates for GSM Evolution) refers to a method in which the available data rates in GSM mobile phone networks are increased by introducing an additional modulation process. With EDGE, GPRS is expanded to become EGPRS (Enhanced GPRS), and HSCSD is expanded to become ECSD.

EGPRS

EGPRS stands for "Enhanced General Packet Radio Service", which describes a packet-oriented data service based on GPRS, which is accelerated by means of EDGE technology.

GPRS

GPRS is the abbreviation for "General Packet Radio Service", a data transmission system of GSM2+ mobile phone systems. GPRS systems use the base stations of GSM networks as their wireless equipment, and their own infrastructure for coupling to other IP networks, such as the Internet. Data communication is packet-oriented; the Internet Protocol (IP) is used. GPRS provides data rates of up to 115.2 kbps.

GSM

GSM (= Global System for Mobile Communication) is a standard that is used worldwide for digital mobile phone networks. In addition to the voice service for telephone calls, GSM supports various data services, such as fax, SMS, CSD and GPRS. Depending on the legal requirements in the various countries, the frequency bands 900 MHz, 1800 MHz or 850 MHz and 1900 MHz are used.

HSPDA, HSUPA (HSPA+)

HSDPA (=High Speed Downlink Packet Access) and HSUPA (=High Speed Upload Packet Access) are extensions of the UMTS network, which provides higher data rates from the base station to the mobile station (HSDPA) or from the mobile station to the base station (HSUPA).

HTTPS

HTTPS (=HyperText Transfer Protocol Secure) is a variant of the familiar HTTP, which is used by any Web browser for navigation and data exchange in the Internet. For example, this familiar entry: http://www.neuhaus.de.

In HTTPS the original protocol is supplemented with an additional component for data protection. While in HTTP data are transmitted unprotected in plain text, in HTTPS data are transmitted only after an exchange of digital certificates, and in encrypted form.

IP address

Every host or router on the Internet / an intranet has a unique IP address (IP = Internet Protocol). The IP address is 32 bits (= 4 bytes) long, and is written as 4 numbers (each in the range from 0 to 255), which are separated from each other by dots.

An IP address has 2 parts: the network address and the host address.

All hosts of a network have the same network address, but different host addresses. Depending on the size of the network in question - a distinction is made between networks of Class A, B and C - the two address components may be of different sizes:

<table>
<tr><td></td><td>1st byte</td><td>2nd byte</td><td>3rd byte</td><td>4th byte</td></tr>
<tr><td>Class A</td><td>Network address</td><td colspan="3">Host address</td></tr>
<tr><td>Class B</td><td colspan="2">Network address</td><td colspan="2">Host address</td></tr>
<tr><td>Class C</td><td colspan="3">Network address</td><td>Host address</td></tr>
</table>

It can be seen from the first byte of the IP address whether the IP address designates a network of Class A, B or C. The following definitions apply:

	Value of the 1st byte	Bytes for the network address	Bytes for the host address
Class A	1-126	1	3
Class B	128-191	2	2
Class C	192-223	3	1

If you do the arithmetic, you can see that there can be a maximum of 126 Class A networks worldwide, and each of these networks can comprise a maximum of 256 x 256 x 256 hosts (3 bytes of address space). There can be 64 x 256 Class B networks, each of which can contain up to 65,536 hosts (2 bytes of address space: 256 x 256). There can be 32 x 256 x 256 Class C networks, each of which can contain up to 256 hosts (1 byte of address space)

IP packet

See Datagram

IPsec

IP security (IPsec) is a standard which uses IP datagrams to ensure the authenticity of the sender, the confidentiality and the integrity of the data through encryption. The components of IPsec are the authentication Header (AH), the encapsulating security payload (ESP), the security association (SA), the security parameter index (SPI) and the internet key exchange (IKE).

At the beginning of the communication, the computers participating in the communication clarify the process used and its implications, such as transport mode or tunnel mode.

In transport mode, an IPsec header is used between the IP header and TCP or UDP header in each IP datagram. Since the IP header remains unchanged in the process, this mode is only suitable for a host-to-host connection.

In tunnel mode, an IPsec header and a new IP header precede the entire IP datagram. That means the original datagram is encrypted in the

payload of the new datagram.

Tunnel mode is used with the VPN: The devices at the tunnel ends encrypt and decrypt the datagrams along the stretch of the tunnel; in other words, the actual datagrams are fully protected along the transport route through the public network.

MIB

See SNMP

NAT (Network Address Translation)

With network address translation (NAT), often called IP masquerading, an entire network is "hidden" behind a single device, known as the NAT router. The internal computers in the local network remain concealed with their IP addresses in the local network when they communicate outwardly through the NAT router. Only the NAT router with its own IP address is visible to outside communication partners.

However, in order for internal computers to be able to communicate directly with external computers (on the internet), the NAT router must change the IP datagrams to and from the internal computer to the outside.

If an IP datagram is sent from the internal network to the outside, the NAT router changes the IP and TCP header of the datagram. It switches the source IP address and the source port with its own official IP address and its own, previously unused port. For this purpose, it maintains a table which establishes the allocation of the original with the new values.

Upon receiving a response datagram, the NAT router recognises that the datagram is actually intended for an internal computer on the basis of the specified target port. Using the table, the NAT router exchanges the target IP address and the target port and forwards the datagram to the internal network.

Network mask / Subnet mask

A company network with access to the Internet is normally officially assigned only a single IP address, e.g. 134.76.0.0. In this example address it can be seen from the 1st byte that this company network is a Class B network, i.e. the last 2 bytes can be used freely for host addressing. Arithmetically that represents an address space of 65,536 possible hosts (256 x 256).

Such a huge network is not very practical. It is necessary here to form subnetworks. This is done using a subnet mask. Like an IP address, this is a field 4 bytes long. The value 255 is assigned to each of the bytes that represent the network address. The main purpose of this is to "hide" a part of the host address range in order to use it for the addressing of subnetworks. For example, in a Class B network (2 bytes for the network address, 2 bytes for the host address), by means of the subnet mask 255.255.255.0 it is possible to take the 3rd byte, which was actually intended for host addressing, and use it now for subnet addressing. Arithmetically that means that 256 subnets with 256 hosts each could be created.

Port number

The Port Number field is a 2-byte field in UDP and TCP headers. The assignment of port numbers serves to identify various data flows that are processed simultaneously by UDP/TCP. The entire data exchange between UDP/TCP and the application processes takes place via these port numbers. The assignment of port numbers to application processes is performed dynamically and randomly. Fixed port numbers are assigned for certain frequently-used application processes. These are called Assigned Numbers.

PPPoE

Acronym for Point-to-Point Protocol over Ethernet. It is based on the standards PPP and Ethernet. PPPoE is a specification for connecting users to the Internet via Ethernet using a jointly used broadband medium such as DSL, Wireless LAN or cable modem.

PPTP

Acronym for Point-to-Point Tunneling Protocol. This protocol was developed by Microsoft, U.S. Robotics and others in order to transmit data securely between two VPN nodes (→ VPN) over a public network.

Private key, public key; certification (X.509)

Two keys are used with asymmetric encryption algorithms: one private (*private key*) and one public (*public key*). The public key is used for the encryption of data and the private key is used for the decryption.

The public key is provided by the future recipient of data to those who encrypt and send data to the recipient. Only the recipient has the private key. It is used for the decryption of the data received.

Certification:

The possibility of certification exists so that the user of the public key (used for encryption) can be certain that the public key really originated from the party who was intended to receive the data to be sent: a certification authority (*CA*) checks the authenticity of the public key and the associated linking of the sender's identity with its key. This is conducted according to the CA's rules, which may require the sender to appear in person. After a successful check, the CA signs the public key of the sender with its (digital) signature. A *certificate* is created.

An X.509 certificate establishes a link between an identity in the form of an "X.500 distinguished name" (DN) and an official key, which is certified with the digital signature of an X.509 certification authority (CA). The signature (an encryption with the signature key) can be checked with the public key which the CA issues to the certificate holder.

Protocol, Transfer protocol

Devices that communicate with each other must use the same rules. They have to "speak the same language". Such rules and standards are called protocols or transfer protocols. Frequently used protocols include IP, TCP, PPP, HTTP and SMTP. TCP/IP is the umbrella term for all protocols that are based on IP.

Service provider

Supplier, company or institution that gives users access to the Internet or to an online service.

Spoofing, Anti-Spoofing

In Internet terminology, spoofing means to specify a forged address. The forged Internet address is used to pose as an authorised user.

Anti-Spoofing means mechanisms to reveal or prevent spoofing.

SNMP

SNMP (Simple Network Management Protocol) is a widespread mechanism for the central control of network components such as servers, routers, switches, printers, computers etc.

SNMP defines the communication process and the structure of the data packages. UDP via IP is used for the transport.

SNMP does not define the values which can be read or changed.

This is done in an MIB (Management Information Base). The MIB is a description file in which the individual values are listed in a table. The MIB is for specific network components or for a class of components, such as switches.

SNMP Trap

SNMP trap is a message which is sent unprompted by the SNMP agent (Simple Network Management Protocol) from a network component.

SSH

SSH (Secure SHell) is a protocol that enables secure, encrypted data exchange between computers. Secure SHell is used for remote access to the input console from LINUX-based machines.

Symmetric encryption

With symmetric encryption, data is encrypted and decrypted with the same key. DES and AES are two examples of symmetric encryption algorithms. They are fast, but time-consuming to administer as the number of users increases.

TACACS+

TACACS+ (**T**erminal **A**ccess **C**ontroller **A**ccess **C**ontrol **S**ystem Plus) is a standardised protocol, which is used for communication between clients and servers within a network in the areas authentication, authorization and accounting (billing). Like the TAINY xMOD, a TACACS+ server can be set up, for example, which manages the access data for all end devices in the network centrally and carries out the authorization for the relevant interested party on behalf of the end devices when registration requests are received. The end device forwards the received registration data to the TACACS+ server, which carries out the necessary checks for the authorization and reports the result of the checks back to the end device.

TCP/IP (Transmission Control Protocol/Internet Protocol

Network protocol that is used to connect two computers on the Internet.

IP is the basic protocol.

UDP builds on IP, and sends individual packets. These can arrive at the recipient in a different sequence from the one they were sent in, or they can even get lost.

TCP serves to secure the connection, and ensures, for example, that the data packets are forwarded to the application in the right sequence.

UDP and TCP provide, in addition to the IP addresses, port numbers between 1 and 65535, which can be used to distinguish the various services.

A number of additional protocols are based on UDP and TCP, such as HTTP (Hyper Text Transfer Protocol), HTTPS (Secure Hyper Text Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol, Version 3), DNS (Domain Name Service).

ICMP builds on IP, and contains control messages.

SMTP is an e-mail protocol based on TCP.

IKE is an IPsec protocol based on UDP.

ESP is an IPsec protocol based on IP.

On a Windows PC, WINSOCK.DLL (or WSOCK32.DLL) handles both of these protocols.

(→ Datagram)

UDP

See TCP/IP

UMTS

UMTS (Universal Mobile Telecommunication System) is a 3rd generation mobile radio network, which allows significant higher data transmission rates, than the 2nd generation GSM networks. UMTS provides beside voice connections also IP-based data connections, SMS transmission and high speed data application like video.

Apart from North America UMTS uses a frequency band at 2100 MHz. In North America the frequency bands at 850 MHz and 1900 MHz are used, which are also used for GSM networks.

VPN (Virtual Private Network)

A virtual private network (VPN) connects several physically separate private networks (subnetworks) through a public network, such as the internet to form a common network. The use of cryptographic protocols ensures confidentiality and authenticity. A VPN thus offers an affordable alternative to standard lines for creating a supraregional company network.

X.509 certificate

A type of "seal" which verifies the authenticity of the public key (→ asymmetric encryption) and corresponding data.

The possibility of certification exists so that the user of the public key (used for encryption) can be certain that the public key really originated

from its actual originator and thus from the party who was intended to receive the data to be sent. A certification authority (CA) checks the authenticity of the public key and the associated linking of the originator's identity with its key. This takes place according to the CA's rules, which may require the originator of the public key to appear in person. After a successful check, the CA signs the public key with its (digital) signature. A certificate is created.

An X.509(v3) certificate thus contains a public key, information about the owner of the key (specified by distinguished name [DN]), allowed purposes of use, etc. and the signature of the CA.

The signature is created as follows: The CA creates an individual bit sequence up to 160 bits long known as the HASH value from the public key's bit sequence, the data on its owner and from additional data. The CA encrypts this with its private key and adds the certificate. Encryption with the CA's private key verifies authenticity, meaning that the encrypted HASH character sequence is the CA's digital signature. If the data of the certificate appears to have been manipulated, this HASH value will no longer be correct and the certificate will be worthless.

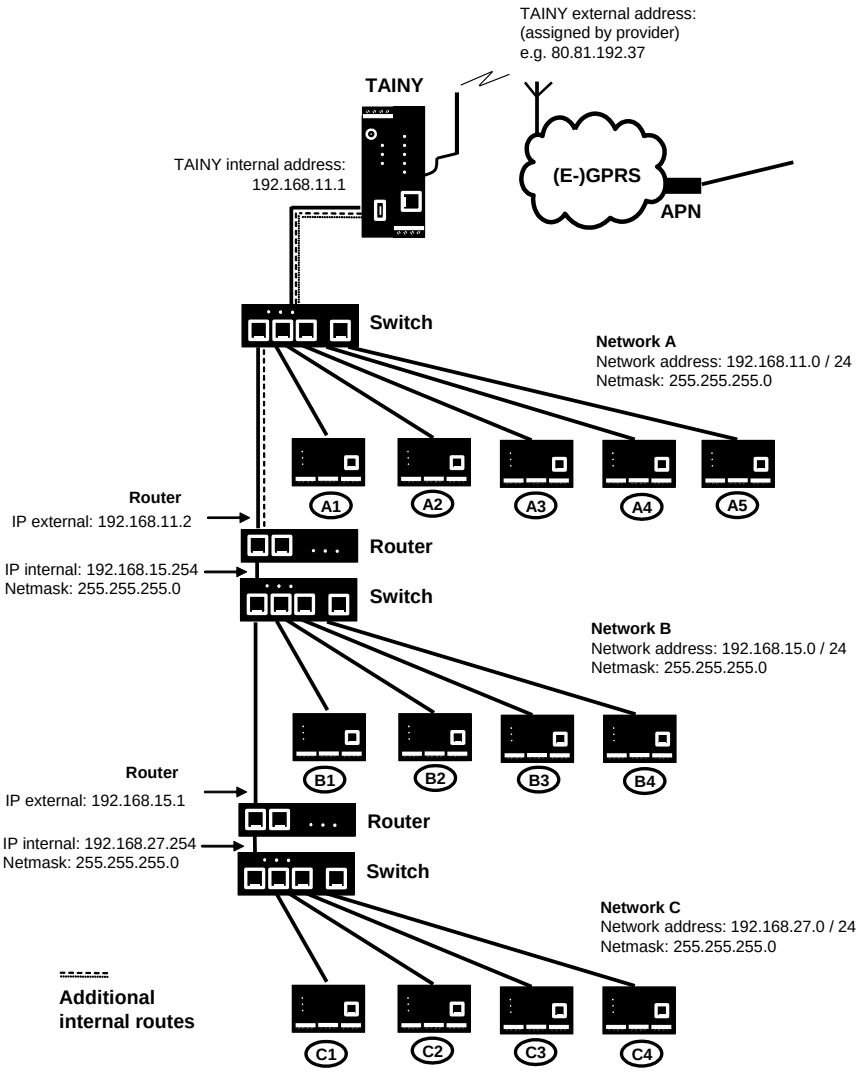
The HASH value is also referred to as a fingerprint. Since it is encrypted with the CA's private key, anyone who has the appropriate public key can encrypt the bit sequence and thus check the authenticity of this fingerprint or this signature.

By using the services of authentication authorities, it is possible that one key owner need not know the other, only the authentication authority. The additional information for the key also simplifies the administrative efforts for the key.

X.509 certificates are used for email encryption, etc. using S/MIME or IPsec.

Additional Internal Routes

The following sketch shows how the IP addresses could be distributed in a local network with subnetworks, what network addresses result from this, and what the specification for an additional internal route could look like.



Network A is connected to the TAINY HMOD-V3-IO and via it to a remote network. Additional internal routes show the path to additional networks (networks B, C), which are connected to each other via gateways (routers). For the TAINY HMOD-V3-IO, in the example shown networks B and C can both be reached via gateway 192.168.11.2 and network address 192.168.11.0/24.

Network A					
Computer	A1	A2	A3	A4	A5
IP address	192.168.11.3	192.168.11.4	192.168.11.5	192.168.11.6	192.168.11.7
Network mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Network B					
Computer	B1	B2	B3	B4	**Additional internal routes:** Network: 192.168.15.0/24 Gateway: 192.168.11.2 Network: 192.168.27.0/24 Gateway: 192.168.11.2
IP address	192.168.15.3	192.168.15.4	192.168.15.5	192.168.15.6	
Network mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	
Network C					
Computer	C1	C2	C3	C4	
IP address	192.168.27.3	192.168.27.4	192.168.27.5	192.168.27.6	
Network mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	

17 Technical data

17.1 TAINY HMOD

Interfaces	Application interface	2-port version: 2x 10/100 Base-T (RJ45 plug) Ethernet IEEE802, 10/100 Mbit/s 5-port version: 5x 10/100 Base-T (RJ45 plug) Ethernet IEEE802, 10/100 Mbit/s
	Service interface	USB-A (reserved for later applications)
Security functions	VPN	VPN IPsec (TAINY HMOD-V3 only) Such as 10 VPN tunnel
	Firewall	Stateful inspection firewall Anti-Spoofing Port forwarding
Additional functions		DNS cache, DHCP server, NTP, remote logging, connection monitoring, alarm-SMS, SNMP, TACACS+
Management		Web-based administration user interface, SSH console
Wireless connection	Frequency bands	UMTS/HSPA+: 800/850, 900, 1900, 2100 MHz GSM/GPRS/EDGE: 850, 900, 1800, 1900 MHz
	HSPA+	HSDPA/HSUPA Data rates: DL: 7.2 / 14.4 Mbps, UL: 2.0 / 5.76 Mbps Concurrent data rate: DL: 7.2 Mbps, UL: 5.76 Mbps
	UMTS	DL: max. 384 kbps, UL: max. 384 kbps
	EDGE (EGPRS)	EDGE class 12: DL: max. 237 kbps, UL: max. 237 kbps
	GPRS	GPRS class 12: DL: max. 85.6 kbps, UL: max. 85.6 kbps
	CSD / MTC	CSD data transmission 14.4 kbps, V.110
	SMS (TX)	Point to point, MO (outgoing)
	Antenna connections	2 connectors: nominal impedance: 50 ohms, jack: SMA
Ambient conditions	Temperature range	Operation: -40 °C to +70 °C *) Storage: -40 °C to +85 °C *) Automatic shut-down of the radio module in case of reaching a critical temperature.
	Air humidity	0-95 %, non-condensing
Housing	Design	Top-hat rail housing
	Material	Plastic
	Protection class	IP20
	Dimensions	2-port version: 114,5 mm x 45 mm x 99 mm 5-port version: 114,5 mm x 67 mm x 99 mm
	Weight	2-port version: ca. 280g 5-port version: ca. 400g

Conformity	CE	Yes
	R&TTE	Conform to directive 99/05/EC Applied standards: EN301 511 v.9.0.2, EN301908-1/-2 v.4.2.1
	HSPA+/UMTS/ GSM/EGPRS-Module	GCF, PTCRB conform
	EMC/ESD	Applied standards: EN 301 489-1 v.1.8.1, EN 301 489-7 v.1.3.1, EN 61000-6-2:2005
	Electrical safety	Applied standards: EN 60950-1:11-2006/A1:2010
	Environment	The device complies with the European Directives RoHS and WEEE.
Power supply	Input voltage	nominal 12-60 VDC, min. -10 %, max +20 %
	Power input	4.4 W typical at 12 V 4.0 W typical at 24 V 5.5 W typical at 60 V
	Supply current	450 mA at 12 V and 100 mA at 60 V I_{Burst}>1.26 A

17.2 TAINY EMOD

Interfaces	Application interface	2-port version: 2x 10/100 Base-T (RJ45 plug) Ethernet IEEE802, 10/100 Mbit/s 5-port version: 5x 10/100 Base-T (RJ45 plug) Ethernet IEEE802, 10/100 Mbit/s
	Service interface	USB-A (reserved for later applications)
Security functions	VPN	VPN IPsec (TAINY EMOD-V3 only)
	Firewall	Stateful inspection firewall Anti-Spoofing Port forwarding
Additional functions		DNS cache, DHCP server, NTP, remote logging, connection monitoring, alarm-SMS, SNMP, TACACS+
Management		Web-based administration user interface, SSH console
Wireless connection	Frequency bands	Quad band: GSM 850/900/1800/1900MHz
	EDGE (EGPRS)	Multislot Class 12 Mobile Station Class B Modulation and Coding Scheme MCS 1 – 9
	GPRS	Multislot Class 12 Full PBCCH support Mobile Station Class B Coding Scheme 1 – 4
	EDGE / GPRS	During data transmission via EGPRS or GPRS the device selects from the following classes: - from EGPRS multislot class 12 (4Tx slots) to EGPRS multislot class 10 (2Tx slots), - from EGPRS multislot class 10 (2Tx slots) to EGPRS multislot class 8 (1Tx), - from GPRS multislot class 12 (4Tx slots) to GPRS multislot class 8 (1Tx) - from GPRS multislot class 10 (2Tx slots) to GPRS multislot class 8 (1Tx)
	CSD / MTC	V.110, RLP, non-transparent 2.4, 4.8, 9.6, 14.4kbps
	SMS (TX)	Point to point, MO (outgoing)
	Max. transmission power (in accordance with output 99, V5)	Class 4 (+33dBm ±2dB) for EGSM850 Class 4 (+33dBm ±2dB) for EGSM900 Class 1 (+33dBm ±2dB) for EGSM850 Class 1 (+30dBm ±2dB) for GSM1900 Class E2 (+27dBm ± 3dB) for GSM 850 8-PSK Class E2 (+27dBm ± 3dB) for GSM 900 8-PSK Class E2 (+26dBm +3 /-4dB) for GSM 1800 8-PSK Class E2 (+26dBm +3 /-4dB) for GSM 1900 8-PSK
	Antenna connection	Nominal impedance: 50 ohms, jack: SMA
Ambient conditions	Temperature range	Operation: -20 °C to +60 °C *) Storage: -40 °C to +85 °C *) Automatic shut-down of the radio module in case of reaching a critical

		temperature.
	Air humidity	0-95 %, non-condensing
Housing	Design	Top-hat rail housing
	Material	Plastic
	Protection class	IP20
	Dimensions	2-port version: 114,5 mm x 45 mm x 99 mm 5-port version: 114,5 mm x 67 mm x 99 mm
	Weight	2-port version: ca. 280g 5-port version: ca. 400g
Conformity	CE	Yes
	R&TTE (GSM)	Conforms to Directive 99/05/EC Applied standard: EN301 511 v.9.0.2
	GSM/EGPRS module	Conforms to GCF, PTCRB
	EMC/ESD	Applied standards: EN 301 489-1 v.1.8.1, EN 301 489-7 v.1.3.1, EN 61000-6-2:2005
	Electrical safety	Applied standard: EN 60950-1:11-2006/A1:2010
	Environment	The device complies with the European Directives RoHS and WEEE.
Power supply	Input voltage	nominal 12-60 VDC, min. -10 %, max +20 %
	Power input	4.4 W typical at 12 V 4.0 W typical at 24 V 5.5 W typical at 60 V
	Supply current	450 mA at 12 V and 100 mA at 60 V I_{Burst}>1.26 A